

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-120300

(43) 公開日 平成11年(1999) 4月30日

(51) Int.Cl.⁶

G 0 6 K 17/00

19/07

識別記号

F I

G 0 6 K 17/00

19/00

B

D

N

審査請求 未請求 請求項の数17 O L (全 42 頁)

(21) 出願番号

特願平9-277817

(22) 出願日

平成9年(1997)10月9日

(71) 出願人 000005223

富士通株式会社

神奈川県川崎市中原区上小田中4丁目1番
1号

(72) 発明者 星野 正雄

神奈川県川崎市中原区上小田中4丁目1番
1号 富士通株式会社内

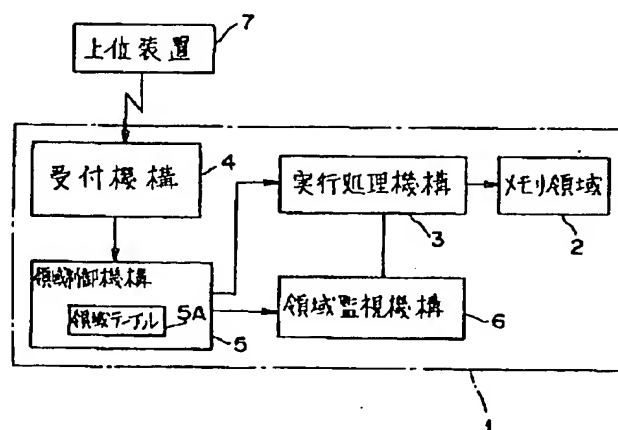
(74) 代理人 弁理士 真田 有

(54) 【発明の名称】 可搬型カード媒体、可搬型カード媒体のメモリ空間管理方法、可搬型カード媒体の発行方法および可搬型カード媒体のプログラムデータ書込方法並びにメモリ空間管理プログラムが記録された本発明の原理ブロック図

(57) 【要約】

【課題】 複数のアプリケーション機能を実現しうる ICカードとして用いられる可搬型カード媒体において、他のアプリケーション機能によって管理されるデータを取り出すことを防止できるようにする。

【解決手段】 上位装置7からのアプリケーション処理依頼を受け付ける受付機構4と、受付機構4にて受け付けられたアプリケーション処理依頼に対応した処理を実行するためのメモリ上の領域2を抽出し、抽出された領域2における実行処理を実行処理機構3に依頼する領域制御機構5と、実行処理機構3にてプログラム実行中にアクセスが発生した領域情報を入力されて、領域制御機構5にて抽出された領域2において、実行処理機構3における処理が実行されているか否かを監視する領域監視機構6とをそなえるように構成する。



【特許請求の範囲】

【請求項 1】 上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、該上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体であって、

該上位装置からの上記アプリケーション処理依頼を受け付ける受付機構と、

該受付機構にて受け付けられたアプリケーション処理依頼に対応した処理を実行するための上記メモリ上の領域を抽出し、上記抽出された領域においての実行処理を該実行処理機構に依頼する領域制御機構と、

該実行処理機構にて上記プログラム実行中にアクセスが発生した領域情報を入力されて、該領域制御機構にて抽出された領域において、該実行処理機構における処理が実行されているか否かを監視する領域監視機構とをそなえて構成されたことを特徴とする、可搬型カード媒体。

【請求項 2】 該領域制御機構が、アプリケーション処理の種別に応じて、該実行処理機構にて処理を実行するための領域情報を予め登録しておく領域テーブルをそなえ、該受付機構にて受け付けられたアプリケーション処理依頼の種別に基づき、該領域テーブルを参照することにより、上記アプリケーション処理依頼に対応した処理を実行するための上記メモリ上の領域を抽出するように構成されたことを特徴とする、請求項 1 記載の可搬型カード媒体。

【請求項 3】 該領域テーブルが、該受付機構にて受け付けられたアプリケーションが使用するデータを記憶するとともに上記プログラムにおけるアクセス制御が動作するアクセス空間に対応する領域を設定するとともに、上記プログラムにおける上記アクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間に対応する領域を設定するように構成されたことを特徴とする、請求項 2 記載の可搬型カード媒体。

【請求項 4】 該領域制御機構が、該受付機構にて受け付けられたアプリケーション処理依頼に対応した処理を実行するための上記メモリ上の領域を、該領域テーブルを参照することにより、アドレス情報またはページ情報により抽出するように構成されたことを特徴とする、請求項 2 記載の可搬型カード媒体。

【請求項 5】 該領域監視機構が、該領域制御機構にて抽出されたメモリ上の領域を登録しておくレジスタ部をそなえ、該レジスタ部にて登録された情報に基づいて、該実行処理機構における処理が実行されているか否かを監視するように構成されたことを特徴とする、請求項 2 記載の可搬型カード媒体。

【請求項 6】 該領域テーブルにおける、該上位装置か

らの上記アプリケーション処理依頼の種別毎に、当該アプリケーション処理依頼の受け付け可否を判定するための認証情報が記憶されたことを特徴とする、請求項 2 記載の可搬型カード媒体。

【請求項 7】 該領域制御機構が、該受付機構にて直前に受け付けられたアプリケーション処理依頼に含まれる、上記アプリケーション処理を識別するための識別情報を、該領域テーブルに登録しておくように構成されたことを特徴とする、請求項 2 記載の可搬型カード媒体。

【請求項 8】 上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、該上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体のメモリ空間管理方法において、

該メモリの領域に対応して、上記アプリケーションが使用するデータを記憶するとともに上記プログラムにおけるアクセス制御が動作するアクセス空間と、上記プログラムにおける上記アクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間と、上記のアクセス空間およびコマンド空間における処理を統括制御する統括制御空間とを設定し、

該統括制御空間において該上位装置からの処理依頼を受けると、該実行処理機構にて上記処理依頼を実行すべく、該統括制御空間から上記のアクセス空間またはコマンド空間に動作を移行させることを特徴とする、可搬型カード媒体のメモリ空間管理方法。

【請求項 9】 複数のアプリケーション処理を行なうべく、該メモリに複数のアプリケーション処理用のプログラムとともに上記プログラム実行の際のデータを記憶する一方、各アプリケーション毎に上記のアクセス空間およびコマンド空間が設定されたことを特徴とする、請求項 8 記載の可搬型カード媒体のメモリ空間管理方法。

【請求項 10】 該アクセス空間において、アクセスできるデータの領域およびアクセス制御が実行できるプログラムの領域を、上記アプリケーション毎に分割して設定することを特徴とする、請求項 9 記載の可搬型カード媒体のメモリ空間管理方法。

【請求項 11】 上記アプリケーション毎に分割して設定されるアクセス空間の一部を、相互に共用化された空間とすることを特徴とする、請求項 10 記載の可搬型カード媒体のメモリ空間管理方法。

【請求項 12】 該コマンド空間において、コマンドが実行できるプログラム領域をアプリケーション単位に分割して設定することを特徴とする、請求項 9 記載の可搬型カード媒体のメモリ空間管理方法。

【請求項 13】 上記アプリケーション毎に分割して設定されるコマンド空間の一部を、相互に共用化された空

間とすることを特徴とする、請求項 1 2 記載の可搬型カード媒体のメモリ空間管理方法。

【請求項 1 4】 該コマンド空間の動作中における該統括制御空間に対する宣言に基づいて、該コマンド空間を拡張させることを特徴とする、請求項 8 記載の可搬型カード媒体のメモリ空間管理方法。

【請求項 1 5】 上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータ

に基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、該上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体を発行する際に、

上記カード媒体を発行しうる該上位装置固有の認証情報を、認証情報を記憶する外部カード媒体に通知する認証情報通知ステップと、

外部カード媒体において、該認証情報通知ステップにて通知された認証情報と、当該外部カード媒体にて記憶される認証情報とを照合、認証し、当該上位装置を介して上記カード媒体の発行可否を判定する照合判定ステップと、

該照合判定ステップにおける判定の結果、上記カード媒体の発行可と判定された場合に、当該上位装置を介して所望のカード媒体を発行する発行ステップとをそなえて構成されたことを特徴とする、可搬型カード媒体の発行方法。

【請求項 1 6】 上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータ

に基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、該上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体の該メモリにプログラムデータを外部装置から書き込む際に、

上記外部装置の認証情報を上記カード媒体に通知するとともに、上記カード媒体の認証情報を上記外部装置に対して通知する認証情報通知ステップと、

上記外部装置において、上記カード媒体から通知された認証情報と当該外部装置にて記憶される認証情報とを照合、認証するとともに、上記カード媒体において、上記外部装置から通知された認証情報と当該カード媒体にて記憶される認証情報とを照合、認証し、当該外部装置から上記プログラムデータの書き込み可否を判定する照合判定ステップと、

該照合判定ステップにおける判定の結果、上記プログラムデータが書き込み可と判定された場合に、上記カード媒体では、上記外部装置を介して書き込み処理を実行する書込処理実行ステップとをそなえて構成されたことを

特徴とする、可搬型カード媒体のプログラムデータ書込方法。

【請求項 1 7】 上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、該上位装置から依頼された所望のアプリケーション処理を実行しうるコンピュータにおいてメモリ空間を管理する際に、

該コンピュータに、

該メモリの領域上に、上記アプリケーションが使用するデータを記憶するとともに上記プログラムにおけるアクセス制御が動作するアクセス空間と、上記プログラムにおける上記アクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間と、上記のアクセス空間およびコマンド空間における処理を統括制御する統括制御空間とを設定する空間設定機能と、

該統括制御空間において該上位装置からの処理依頼を受けると、該実行処理機構にて上記処理依頼を実行すべく、該統括制御空間から上記のアクセス空間またはコマンド空間に動作を移行させる空間制御機能とを実現させるためのメモリ空間管理プログラムが記録されたことを特徴とする、メモリ空間管理プログラムが記録されたコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】 (目次)

発明の属する技術分野

従来の技術 (図 2 3)

発明が解決しようとする課題

課題を解決するための手段 (図 1)

発明の実施の形態 (図 2 ~ 図 2 2)

発明の効果

【0002】

【発明の属する技術分野】 本発明は、複数のアプリケーション機能を実現しうる IC (Integrated Circuit) カードとして用いて好適な、可搬型カード媒体に関するとともに、この可搬型カード媒体のメモリ空間管理方法、発行方法およびプログラムデータ書込方法に関し、さらに、メモリ空間管理プログラムが記録されたコンピュータ読取可能な記録媒体に関するものである。

【0003】

【従来の技術】 IC カードは、従来よりの磁気記録カードよりも大量のデータを記憶しうる集積回路 (IC; Integrated Circuit) が埋め込まれた可搬性を有するカード媒体であって、個人が所有する個人データ等を記録しておくものである。これにより、IC カードを上位装置に接続することで、上述の磁気記録カードよりも発展したアプリケーション処理を実現できるようになっている。

【0004】 すなわち、上述したように、この IC カー

ドは、磁気記録カードよりも記憶容量が大きいことはもとより、記録される個人情報のセキュリティ機能（個人情報等の機密保持機能）を向上させることができるようになっている。ここで、図23に示すように、ICカード100は、CPU(Central Processing Unit)101をそなえると同時に、カード外部とのインタフェース機能を有するコネクタ部102およびデータ記憶用のメモリ103をそなえて構成されている。なお、メモリ103としては、例えば消去書込可能ROM(EPROM)が用いられる。

【0005】CPU101は、CPU101を駆動するためのプログラムを記憶する読み出し専用化されたメモリ(ROM:Read Only Memory)101a、プログラム実行の際に用いられるデータを格納しておくRAM(Random Access Memory)101b、ROM101aに記録されたプログラムに従って各種コマンド処理等の制御処理を行なう制御部101cおよびデータに関する演算処理を行なう演算部101dをそなえて構成されている。

【0006】近年においては、このようなICカードを利用することにより、現金に代わる電子マネーのシステム開発が活発に行なわれている。このような電子マネーのシステムについての実験的試行は、各所において実施されており、実運用段階にまで急速に進展しつつある。ここで、電子マネーシステムは、例えば銀行の自動取引装置(ATM)などを介することにより、ユーザの所有するICカードに、現金と同様の電子的な金銭情報（ユーザが所持する金額情報）が移動されて、この金銭情報を用いることにより、対価としての金銭情報を相手方に移動させる処理を行なうシステムであり、このシステムにより、現金の授受やクレジット処理などを伴わずに現実

に各種商取引を行なうことができる。

【0007】ところで、このICカード100は、通常は、一枚のカード内に上述のごとき電子マネーとしての単一のアプリケーション機能のみをそなえて用いられているが、近年のICカードにおける集積回路内のメモリの記憶容量や、CPU(Central Processing Unit)の処理速度の向上に伴って、複数のアプリケーション機能を持たせて使用することも考えられている。

【0008】ここで、一枚のカード内に単一のアプリケーション機能のみを動作させて用いる場合には、ICカード100のROM101aに、当該アプリケーション機能を実現させるためのプログラムをハードウェアに予め書き込んでおくタイプのものが用いられている。一方で、上述のごとき複数のアプリケーション機能（マルチアプリケーション機能）を持たせてICカードを使用する場合には、ユーザが使用するアプリケーションを任意に選択できるようにすべく、アプリケーション機能を実現させるためのプログラムをユーザ側でローディングできるようにすることが考えられている。

【0009】すなわち、各ユーザにおいてICカードを

利用する前段において、ユーザ自身で所望のアプリケーション機能を実現するプログラムをICカードに書き込ませた後に（ローディングさせた後に）、多機能ICカードとして利用できるようにしているのである。

【0010】

【発明が解決しようとする課題】しかしながら、上述のごとき複数のアプリケーション機能を実現しようとする可搬型カード媒体としてのICカードにおいては、各プログラムにて処理、管理されるデータを単一のメモリ103において記憶するようになっているため、あるプログラムにて管理されるデータが、他のプログラムによるアクセスにより取り出されてしまうことが考えられ、この場合には記憶されているデータの機密性を保全することが困難であるという課題がある。

【0011】本発明は、このような課題に鑑み創案されたもので、記憶されているデータのセキュリティ機能を保全すべく、アプリケーション機能を実現するプログラムを動作させる際に、CPUの動作領域を予めメモリ上に制限的に設定しておくことにより、他のアプリケーション機能によって管理されるデータを取り出すことを防止できるようにした、可搬型カード媒体とともに、この可搬型カード媒体のメモリ空間管理方法、発行方法およびプログラムデータ書込方法、さらに、メモリ空間管理プログラムが記録されたコンピュータ読取可能な記録媒体を提供することを目的とする。

【0012】

【課題を解決するための手段】図1は本発明の原理ブロック図であり、この図1において、1は可搬型のカード媒体であり、この可搬型カード媒体1においては、上位装置7からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリ領域2に記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構3にて行なうことにより、上位装置7から依頼された所望のアプリケーション処理を実行しうるものであり、受付機構4、領域制御機構5および領域監視機構6をそなえている。

【0013】ここで、受付機構4は、上位装置7からの上記アプリケーション処理依頼を受け付けるものであり、領域制御機構5は、受付機構4にて受け付けられたアプリケーション処理依頼に対応した処理を実行するための上記メモリ2上の領域を抽出し、上記抽出された領域においての実行処理を実行処理機構3に依頼するものである。

【0014】さらに、領域監視機構6は、実行処理機構3にて上記プログラム実行中にアクセスが発生した領域情報を入力されて、領域制御機構5にて抽出された領域において、実行処理機構3における処理が実行されているか否かを監視するものであり（請求項1）、領域テーブル5Aをそなえている。ここで、領域テーブル5A

10

20

30

40

50

は、アプリケーション処理の種別に応じて、実行処理機構3にて処理を実行するための領域情報を予め登録しておくものであり、領域制御機構5では、受付機構4にて受け付けられたアプリケーション処理依頼の種別に基づき、領域テーブル5Aを参照することにより、上記アプリケーション処理依頼に対応した処理を実行するための上記メモリ2上の領域を抽出するようになっている（請求項2）。

【0015】さらに、受付機構4にて受け付けられたアプリケーションが使用するデータを記憶するとともに上記プログラムにおけるアクセス制御が動作するアクセス空間に対応する領域を設定するとともに、上記プログラムにおける上記アクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間に対応する領域を設定するように、領域テーブル5Aを構成することができる（請求項3）。

【0016】また、受付機構4にて受け付けられたアプリケーション処理依頼に対応した処理を実行するための上記メモリ2上の領域を、領域テーブル5Aを参照することにより、アドレス情報またはページ情報により抽出するように、領域制御機構5を構成してもよい（請求項4）。さらに、領域制御機構5にて抽出されたメモリ2上の領域を登録しておくレジスタ部をそなえ、レジスタ部にて登録された情報に基づいて、実行処理機構における処理が実行されているか否かを監視するように、領域監視機構6を構成することもできる（請求項5）。

【0017】また、領域テーブル5Aにおいては、上位装置7からの上記アプリケーション処理依頼の種別毎に、当該アプリケーション処理依頼の受け付け可否を判定するための認証情報を記憶してもよい（請求項6）。また、領域制御機構5を、受付機構4にて直前に受け付けられたアプリケーション処理依頼に含まれる、上記アプリケーション処理を識別するための識別情報を、領域テーブル5Aに登録しておくように構成することもできる（請求項7）。

【0018】さらに、本発明の可搬型のカード媒体のメモリ空間管理方法は、上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体のメモリ空間管理方法において、メモリの領域に対応して、上記アプリケーションが使用するデータを記憶するとともに上記プログラムにおけるアクセス制御が動作するアクセス空間と、上記プログラムにおける上記アクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間と、上記のアクセス空間およびコマンド空間における処理を統括制御する統括制御空間とを設

定し、統括制御空間において上位装置からの処理依頼を受けると、実行処理機構にて上記処理依頼を実行すべく、統括制御空間から上記のアクセス空間またはコマンド空間に動作を移行させることを特徴としている（請求項8）。

【0019】この場合においては、複数のアプリケーション処理を行なうべく、メモリに複数のアプリケーション処理用のプログラムとともに上記プログラム実行の際のデータを記憶する一方、各アプリケーション毎に上記のアクセス空間およびコマンド空間を設定することができる（請求項9）。さらに、メモリ媒体のメモリ空間管理方法は、アクセス空間において、アクセスできるデータの領域およびアクセス制御が実行できるプログラムの領域を、上記アプリケーション毎に分割して設定することができ（請求項10）、この場合においては、上記アプリケーション毎に分割して設定されるアクセス空間の一部を、相互に共用化された空間とすることができる（請求項11）。

【0020】また、コマンド空間において、コマンドが実行できるプログラム領域をアプリケーション単位に分割して設定することができるほか（請求項12）、上記アプリケーション毎に分割して設定されるコマンド空間の一部を、相互に共用化された空間とすることもできる（請求項13）。また、コマンド空間の動作中における統括制御空間に対する宣言に基づいて、コマンド空間を拡張させることができる（請求項14）。

【0021】さらに、本発明の可搬型カード媒体の発行方法は、上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体を発行する際に、上記カード媒体を発行しうる上位装置固有の認証情報を、認証情報を記憶する外部カード媒体に通知する認証情報通知ステップと、外部カード媒体において、認証情報通知ステップにて通知された認証情報と、当該外部カード媒体にて記憶される認証情報とを照合、認証し、当該上位装置を介して上記カード媒体の発行可否を判定する照合判定ステップと、照合判定ステップにおける判定の結果、上記カード媒体の発行可と判定された場合に、当該上位装置を介して所望のカード媒体を発行する発行ステップとをそなえ、上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体を発行することを特徴としている（請求項15）。

【0022】また、本発明の可搬型カード媒体のプログラムデータ書込方法は、上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラム

とともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、上位装置から依頼された所望のアプリケーション処理を実行しうる可搬型のカード媒体のメモリにプログラムデータを外部装置から書き込む際に、上記外部装置の認証情報を上記カード媒体に通知するとともに、上記カード媒体の認証情報を上記外部装置に対して通知する認証情報通知ステップと、上記外部装置において、上記カード媒体から通知された認証情報と当該外部装置にて記憶される認証情報とを照合、認証するとともに、上記カード媒体において、上記外部装置から通知された認証情報と当該カード媒体にて記憶される認証情報とを照合、認証し、当該外部装置から上記プログラムデータの書き込み可否を判定する照合判定ステップと、照合判定ステップにおける判定の結果、上記プログラムデータが書き込み可と判定された場合に、上記カード媒体では、上記外部装置を介して書き込み処理を実行する書込処理実行ステップとをそなえて構成されたことを特徴としている（請求項 16）。

【0023】また、本発明のメモリ空間管理プログラムが記録されたコンピュータ読取可能な記録媒体は、上位装置からの各種アプリケーション処理依頼に対応して実行すべき複数のプログラムとともに上記各プログラム実行の際のデータをメモリに記憶するとともに、上記記憶された各プログラムおよびデータに基づいて、上記各プログラムの実行処理を実行処理機構にて行なうことにより、上位装置から依頼された所望のアプリケーション処理を実行しうるコンピュータにおいてメモリ空間を管理する際に、コンピュータに、メモリの領域上に、上記アプリケーションが使用するデータを記憶するとともに上記プログラムにおけるアクセス制御が動作するアクセス空間と、上記プログラムにおける上記アクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間と、上記のアクセス空間およびコマンド空間における処理を統括制御する統括制御空間とを設定する空間設定機能と、統括制御空間において上位装置からの処理依頼を受けると、実行処理機構にて上記処理依頼を実行すべく、統括制御空間から上記のアクセス空間またはコマンド空間に動作を移行させる空間制御機能とを実現させるためのメモリ空間管理プログラムが記録されたことを特徴としている（請求項 17）。

【0024】

【発明の実施の形態】以下、図面を参照することにより本発明の実施の形態について説明する。

（A）本実施形態にかかる IC カードの概略的構成および適用態様の説明

まず、本実施形態にかかる IC カードの概略的構成とともに、IC カードの適用態様について説明する。

【0025】図 2 は本発明の一実施形態にかかる IC

（IC: Integrated Circuit）カードを示すブロック図であるが、この図 2 に示す IC カード 10 は、前述したように、大量のデータを記憶しうる集積回路が埋め込まれた可搬性あるいは携帯性を有する可搬型カード媒体を構成するものであって、例えば複数のアプリケーションを実現するために共用して用いることができるようになっている。

【0026】すなわち、本実施形態にかかる IC カード 10 は、例えば図 3 に示すように、電子マネーや医療情報のアプリケーションシステム等における複数種類の上位装置に同一カードを接続することにより、各種アプリケーションシステムを実現することができる、いわゆるマルチアプリケーションシステムを構築できるようになっている。

【0027】ここで、本実施形態にかかる IC カード 10 は、図 2 に示すように、ハードウェア的には CPU (Central Processing Unit) 20 およびデータ記憶用のメモリ 30 をそなえるとともに、カード外部とのインタフェース機能を有する図示しないコネクタ部をそなえている。メモリ 30 は、上位装置 40 からの各種アプリケーション処理依頼に対応して、CPU 20 にて実行すべき複数のプログラムとともに上記各プログラム実行の際のデータを記憶するものであり、このメモリ 30 にて記憶される各種アプリケーション処理用のプログラムは、カード製造時に予め書き込まれた書き換え不可のメモリや、使用者の用途に応じて後からローディングしうる書込可能なメモリを用いて記憶させることもできる。

【0028】また、メモリ 30 の領域は、記憶されるデータの性質に応じ、統括制御領域 30A、データ領域 30B およびプログラム領域 30C の 3 つに分割されている。ところで、この IC カード 10 は、図示しないコネクタ部が接続された上位装置 40 からの処理要求に対して、IC カード 10 内に記憶されたプログラムが動作することにより、各種アプリケーション動作を実現することができるようになっている。なお、上述のアプリケーション動作は、IC カード 10 内に記憶されたプログラムのほかに、上位装置 40 内に記憶されたプログラムを協働して動作させながら実現することもできる。

【0029】これにより、例えば図 3 に示すように、カード発行装置 15、16 において予め電子マネーおよび医療情報のアプリケーション等、複数のアプリケーションのためのソフトウェアのローディング処理や、使用者が持つ後述の認証情報を登録すること等を通じて、IC カード 10 の発行処理（カード発行処理）を行ない、発行された IC カード 10 を用いて複数のアプリケーションシステムに共用して適用することができるのである。

【0030】ここで、上述のごとく、電子マネーのアプリケーションシステムにおける IC カード 10 の使用態様としては、カード発行装置 15 にてカード発行された IC カード 10 を、例えば銀行の自動取引装置（AT

M) 11に接続することで、現金と同様の電子的な金銭情報(ユーザが所持する金額情報)をICカード10に蓄積したり、現金口座に入金したりすることができるようになっているほか、ICカード10に入金された金銭情報を用いることにより、パーソナルコンピュータ(PC)やPOS(Point Of Sales)等の端末12を介して支払い処理を電子的に行なうことができる。

【0031】すなわち、この電子マネーのアプリケーションシステムにより、商品の対価としての金銭情報を電子的な情報とし、ICカード10および端末12を介して相手方に移動させることにより、現金の授受を伴わない各種商取引を、クレジット方式を採用せずに現実に行なうことができるのである。また、医療情報のアプリケーションシステムにおいては、例えば使用者が病院への診療に出向いた際に、カード発行装置16にてカード発行されたICカード10に、心電図計等の医療機14を通じての診療情報(心電図計の場合には測定結果)を電子的に記録し、必要に応じて証明書発行機13にICカード10を接続することにより、医療機14による診断証明書等を発行することができるようになっている。

【0032】(B)本実施形態にかかるICカードの機能についての説明

ところで、本実施形態にかかるICカード10においては、上述のごとく複数のアプリケーションシステムに共用して適用することができるようになっているが、あるアプリケーションで管理されるデータを、他のアプリケーションにより取り出されることを防止すべく、CPU20によるメモリ上の動作領域を、その動作状態に応じて制限的に設定するようになっている。

【0033】このため、本実施形態にかかるICカード10は、この図2に示すように、命令実行部21、受付部22、領域制御部23および領域監視部24をそなえて構成されている。なお、上述の命令実行部21、受付部22、領域制御部23および領域監視部24としての機能は、ICカード10内のハードウェア、ソフトウェア資源を適宜使用することにより実現される。換言すれば、これらの各機能部による機能は、CPU20のメモリ30へのアクセス等を通じ、メモリ30内に記憶されたプログラムが動作することで実現される。

【0034】また、これらの各機能(符号21~24参照)を実現するためのプログラム(メモリ空間管理プログラム)は、例えばCD-ROM等の記録媒体に記録されたものからローディングするようにしてもよい。ここで、命令実行部21は、ハードウェア的にはCPU20により構成され、メモリ30に記憶された各種アプリケーション処理のためのプログラムおよびデータに基づいて、これら各プログラムの実行処理を行なって、上位装置40から依頼された所望のアプリケーション処理を実行しうるものであり、実行処理機構として機能する。

【0035】また、受付部22は、図示しないコネクト

部を介して接続された上位装置40からのアプリケーション処理依頼を受け付けるものであり、受付機構としての機能を有している。さらに、領域制御部23は、受付部22にて受け付けられたアプリケーション処理依頼に対応した処理を実行するためのメモリ30上の領域を抽出し、抽出された領域においての実行処理を命令実行部21に依頼するものであり、領域制御機構としての機能を有している。

【0036】すなわち、アプリケーション処理の種別に応じて命令実行部21にて処理を実行するための領域情報を予め登録しておく空間テーブル(領域テーブル)23aを統括制御領域30Aにそなえている。換言すれば、上述の空間テーブル23aに関する情報は、メモリ30における統括制御領域30Aに記憶される。すなわち、上述の領域制御部23としての機能は、CPU20にて領域30A内の空間テーブル23aに関する情報を読み出すことを通じて実現される。

【0037】ここで、空間テーブル23aには、後述の図9に示すように、受付部22にて受け付けられたアプリケーション処理用のプログラムにおけるアクセス制御が動作するアクセス空間32が設定されるとともに、このプログラムにおけるアクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間33が設定されるようになっている。

【0038】すなわち、空間テーブル23aは、後述の図10に示すように、アプリケーションの種別毎に、受付部22にて受け付けられたアプリケーションが使用するデータ32B-1、32B-2と、アプリケーション処理の際のアクセス制御を行なうためのプログラムとを記憶するメモリ30上の領域32C-1、32C-2とをアクセス空間として設定するようになっている。

【0039】さらに、空間テーブル23aは、後述の図11に示すように、アプリケーションの種別毎に、このアプリケーション処理の際のアクセス制御以外、例えばデータを創成するコマンド(発行コマンド)や、上位装置40のアプリケーションから要求される処理を実行するためのコマンドが記憶されたメモリ30上の領域33C-1、33C-2をコマンド空間として設定するようになっている。

【0040】これにより、領域制御部23では、上述の空間テーブル23aを参照することにより、受付部22にて受け付けられたアプリケーション処理依頼の種別に基づき、上位装置40からのアプリケーション処理依頼に対応した処理を実行するためのメモリ30上の領域を抽出することができるようになっている。なお、領域制御部23では、抽出された領域情報について後段の領域監視部24のコントロールレジスタ24aに設定したのち、命令実行部21に対して抽出されたメモリ30の領域情報を通知することにより、当該領域情報に記憶されたプログラムに従って処理が行なわれるようにすべく依

頼する。

【0041】また、領域監視部24は、命令実行部21にて上述のプログラム実行中にメモリ30に対するアクセスが発生した領域情報を入力されて、領域制御部23にて抽出された領域において、命令実行部21における処理が実行されているか否かを監視するものであり、領域監視機構としての機能を有している。具体的には、領域監視部24は、領域制御部23にて抽出された領域情報をハードウェア的に設定しておくコントロールレジスタ24aをそなえて構成され、命令実行部21にて発生するメモリアccessのアドレスが、コントロールレジスタ24aにて設定された領域情報内のアドレス（あるいはページ）か否かを判定するようになっている。

【0042】換言すれば、コントロールレジスタ24aは、領域制御部23にて抽出されたメモリ30上の領域を登録しておくレジスタ部として機能し、領域制御部24では、このコントロールレジスタ24aにて登録された情報に基づき命令実行部21における処理が実行されているか否か、すなわち、命令実行部21における処理が領域制御部23にて抽出された領域内で実行されているか否かを監視することができるのである。

【0043】(C)本実施形態にかかるICカードの動作空間の説明

次に、本実施形態にかかるICカード10の動作空間について説明する。上述したように、本実施形態にかかるICカード10のメモリ30の領域は、記憶されるデータの性質に応じ、統括制御領域30A、データ領域30Bおよびプログラム領域30Cの3つに分割されている。

【0044】また、各アプリケーションのプログラムやデータは、それぞれデータ領域30Bおよびプログラム領域30C内に記憶されている。具体的には、図4に示すように、電子マネーアプリケーションのプログラムで用いるデータ（ファイルを含む）および医療情報アプリケーションのプログラムで用いるデータ（ファイルを含む）は、データ領域30B内に記憶され、電子マネーのアプリケーションのためのプログラムおよび医療情報のアプリケーションのためのプログラムは、プログラム領域30C内に記憶される。

【0045】なお、上述の各アプリケーションのためのプログラムは、ともに上位装置40で要求されるコマンド情報、メモリ30上のデータをアクセスするアクセス制御情報、データを創成する発行コマンド情報のほか、各種データなどにより構成される。ここで、統括制御領域としての統括制御領域30Aには、上述の各アプリケーションを実行するための動作領域（CPU20のアクセス先としての領域30B、30C）を、アプリケーション種別に応じて統括的に監視・制御するためのプログラムとしてのOS(Operating System)を記憶するものある。

【0046】また、CPU20はメモリ30の所定領域を必要に応じてアクセスすることを通じて、所望のアプリケーション処理を実現するようになっているが、このCPU20の実行態様に応じた動作領域を、メモリ30上の領域に対応した3種類の空間で設定することができるようになっている。具体的には、図8または図9に示すように、CPU20の動作領域を、メモリ30の領域に対応して、OS空間31、アクセス空間32およびコマンド空間33と設定することができる。

【0047】ここで、アクセス空間32は、CPU20がアクセス制御を行なっている際に動作するメモリ30上の領域を示すものである。すなわち、このアクセス空間32には、上述の各アプリケーションが使用するデータを記憶するとともに各アプリケーションのためのプログラムにおけるアクセス制御情報が記憶されており、メモリ30におけるデータ領域30Bおよびプログラム領域30Cを構成するアクセス制御プログラムに相当する領域に対応している。

【0048】また、コマンド空間33は、例えば“Create”, “Read”, “Write”等、上述の各プログラムにおけるアクセス制御以外のコマンド（データを創成する発行コマンドを含む）が動作するメモリ30上の領域を示すものである。すなわち、このコマンド空間33には、プログラム領域30Cにおけるアクセス制御プログラム以外のコマンド情報が記憶されている。

【0049】したがって、CPU20によるプログラム実行中、コマンド実行の際にはコマンド空間33で動作し、アクセス制御の際にはアクセス空間32で動作するようになっているが、これらアクセス空間32およびコマンド空間33による動作については、OS空間31で監視・制御されるようになっている。すなわち、OS空間31は、CPU20が上述の統括制御領域30Aに記憶されたプログラム（OS、図2の符号21～24に示す各機能を参照）に基づいた動作状態にある際の、アクセス可能なメモリ30上の領域を示すもので、メモリ30上の全ての領域により構成される。

【0050】すなわち、OS空間31は、統括制御領域30Aに記憶されたプログラムが動作している状態においては、CPU20は、統括制御領域30A、データ領域30Bおよびプログラム領域30Cのすべてに対しアクセスできるようになっている。換言すれば、このOS空間31は、アクセス空間32およびコマンド空間33における処理を統括して監視・制御するための空間で、統括制御空間として機能する。

【0051】具体的には、OS空間31は、後述するように、上位装置40からのアプリケーションの処理依頼を受けると、そのアプリケーションの種別および対応するプログラムに従って、OS空間31からアクセス空間32またはコマンド空間33のいずれかに移行させることができるようになっている。換言すれば、OS空間3

1における動作状態においては、上位装置40からのアプリケーションの処理依頼に基づいて、アクセス可能なメモリ30の領域を制限的に設定しながら、対応するプログラムの実行処理に移行すべく制御することができるのである。

【0052】ところで、上述の2つのアプリケーションを実現するためのそれぞれのプログラムおよびデータは、メモリ30において互いに異なる領域に記憶されるようになっている。従って、複数のアプリケーション処理を行なうべく、メモリ30に複数のアプリケーション処理用のプログラムとともに、これら複数のアプリケーション処理用のプログラムを実行する際のデータを記憶する一方、各アプリケーション毎にアクセス空間32およびコマンド空間33を設定することを通じ、メモリ管理を行なうことができる。

【0053】さらに、アクセス空間32においては、アクセスできるデータの領域およびアクセス制御が実行できるプログラムの領域を、アプリケーション毎に分割して設定することができるほか、コマンド空間33において、コマンドが実行できるプログラム領域をアプリケーション単位に分割して設定することもできる。具体的には、アクセス空間32に対応するメモリ30上の2組のデータおよびアクセス制御情報は、例えば図10に示すような互いに異なったアドレス領域で記憶される。すなわち、電子マネーアプリケーションのアクセス空間は、データ領域30Bにおける前半の領域32B-1とプログラム領域30Cの前半の領域32C-1とで構成される。

【0054】同様に、医療情報アプリケーションのアクセス空間は、データ領域30Bにおける後半の領域32B-2とプログラム領域30Cの領域32C-1に続く領域32C-2とで構成される。さらに、コマンド空間33に対応するメモリ30上の2組のプログラムは、例えば図11に示すように、互いに異なるアドレス領域で記憶される。すなわち、電子マネーアプリケーションのコマンド空間は、プログラム領域30C上の領域33C-1により構成され、医療情報アプリケーションのコマンド空間は、プログラム領域30Cの領域33C-2により構成される。

【0055】ところで、上述のコマンド空間33を構成する2組のプログラムのうちで、OS領域31の制御に基づき、例えば図12（または図8）に示すように、コマンド空間33を拡張（領域を拡大）させることもできる。換言すれば、コマンド空間33の動作中におけるOS空間30Aに対する宣言に基づいて、コマンド空間33を拡張させることができる。

【0056】すなわち、この図8または図12に示すように、CPU20が電子マネーアプリケーションのコマンド空間としての領域33C-1において動作中に、“return”等のコマンドを「拡張宣言」として動作がOS空

間31に移行すると、このOS空間31によりコマンド空間が拡張する。これにより、電子マネーアプリケーションのコマンド空間は、領域33C-1から領域33C-11となる。

【0057】これにより、例えば認証情報の照合の際に、プログラム開発者と認証された使用者以外の使用者が書き込みできない領域をブラックボックスとしての拡張領域として設定しておけば、同一アプリケーションの一部で機密処理（ブラックボックス）することも可能であり、プログラムの改ざんや、認証情報を照合するための暗号アルゴリズムやキー若しくは暗号処理の改ざんを防止することができる。

【0058】さらに、上述の2つのアプリケーション（電子マネーおよび医療情報）間における各アクセス空間において、データあるいはアクセス制御情報を共有できる場合には、同一の領域で記憶することができるようになっている。換言すれば、ICカード10においては、アプリケーション毎に分割して設定されるアクセス空間の一部を、相互に共用化された空間とすることができる。

【0059】例えば図8または図13に示すように、上述の2つのアプリケーション（電子マネーおよび医療情報）における各アクセス空間に対応するデータのうちで、共有しうるものについては、共用データ領域32B-3に記憶される一方、互いに共有しないものについては、それぞれ領域32B-1、32B-2に記憶されるようになっている。

【0060】同様に、上述の2つのアプリケーション（電子マネーおよび医療情報）における各アクセス空間に対応するアクセス制御情報のうちで、共有しうるものについては、共用アクセス制御領域32C-3に記憶される一方、互いに共有しないものについては、それぞれ領域32C-1、32C-2に記憶されるようになっている。

【0061】また、上述の2つのアプリケーション（電子マネーおよび医療情報）間における各コマンド空間において、コマンドを共有できる場合には、同一の領域で記憶することができるようになっている。換言すれば、ICカード10においては、アプリケーション毎に分割して設定されるコマンド空間の一部を、相互に共用化された空間として、メモリ30を管理することもできるのである。

【0062】例えば図14に示すように、上述の2つのアプリケーション（電子マネーおよび医療情報）における各アクセス空間に対応するコマンド情報のうちで、共有しうるものについては、共用コマンド領域33C-3にて記憶する一方、互いに共有しないものについては、それぞれ領域33C-1、33C-2にて記憶するようになっている。

【0063】なお、図14に示す共用コマンド領域33

C-3を拡張する場合には、例えば図8に示すように、OS空間31からの「拡張宣言」によりコマンド空間を拡張させて、共用拡張コマンド領域33C-31とすることが出来る。

(D) 本実施形態にかかる空間テーブルおよびコントロールレジスタの構成の説明

ところで、領域制御部23では、例えば図5に示すような空間テーブル23aを参照することにより、受付部22にて受け付けられたアプリケーション処理依頼に対応した処理を実行するためのメモリ30上の領域を抽出し、抽出された領域においての実行処理を命令実行部21に依頼することを通じて、CPU20の動作状態を、OS空間31から、アクセス空間32またはコマンド空間33のいずれかとするようにしている。

【0064】ここで、この図5に示す空間テーブル23aは、アプリケーション識別情報(AID: Application Identification) 41、ポイント情報42、ステータス情報43、認証情報44、コマンド空間領域情報45、テーブルポイント情報46、アクセス空間領域情報47およびテーブルポイント情報48をそなえて構成されている。

【0065】AID41は、アプリケーション種別毎に、そのアプリケーションを識別するための情報、すなわち、受付部22にて直前に受け付けられたアプリケーション処理依頼に含まれる、アプリケーション処理を識別するための識別情報である。また、ポイント情報42は、後述する共用空間テーブル23a-1にポイントするための情報であり、ステータス情報43は、ID情報41に対応するアプリケーションが動作状態であるか否かを示すとともに、この空間テーブル23a上において登録されるアクセス空間およびコマンド空間をメモリ30上の領域で指定する際の方式について示すものである。

【0066】具体的には、このステータス情報43には、現在CPU20において該当アプリケーションが実行されている状態の場合には、アクティブ“A”を設定するとともに、上述のアクセス空間およびコマンド空間を示すメモリ30上の開始位置および終了位置を、アドレス情報で指定する場合には“AD”を、ページ情報で指定する場合には“PG”を、それぞれ設定するようになっている。

【0067】また、認証情報44は、後述する拡張アドレスを用いた処理を行なう際に必要な上位装置40の使用者の認証情報を照合するためのものであり、この認証情報の照合を通じて、上位装置40の使用者が、メモリ30上の拡張アドレス空間にアクセスできる資格を有しているか否かを判定することができる。換言すれば、空間テーブル23aは、上位装置40からのアプリケーション処理依頼の種別毎に、当該アプリケーション処理依

頼の受け付け可否を判定するための認証情報44を記憶するようになっている。

【0068】さらに、コマンド空間領域情報45は、ID情報41に対応するアプリケーションにおけるコマンド空間を、メモリ30上の領域情報により示すものである。また、このコマンド空間領域情報45は、コマンド空間としてのメモリ30上の領域を、領域の開始位置情報と終了位置情報とで設定(指定)するものであり、これら開始位置および終了位置の情報としては、例えばアドレス情報を用いることができる。

【0069】具体的には、コマンド空間領域情報45としては、通常のコマンド情報を記憶するメモリ領域の開始アドレスおよび終了アドレスが登録されたコマンド空間情報45aをそなえるとともに、拡張されたコマンド空間についてのメモリ30上の開始アドレスおよび終了アドレスが登録された拡張コマンド空間情報45bをそなえている。

【0070】さらに、アクセス空間領域情報47は、ID情報41に対応するアプリケーションにおけるアクセス空間を、メモリ30上の領域情報により示すものである。また、このアクセス空間領域情報47は、アクセス空間としてのメモリ30上の領域を、領域の開始位置情報と終了位置情報とにより設定されたものであり、これら開始位置および終了位置の情報についても、例えばアドレス情報を用いることができる。

【0071】具体的には、アクセス空間領域情報47としては、アクセス対象のデータ領域についてのメモリ30上の開始アドレスおよび終了アドレスが登録されたデータ空間情報47aをそなえるとともに、アクセス制御情報についてのメモリ30上の開始アドレスおよび終了アドレスが登録されたアクセス制御空間情報47bをそなえている。

【0072】また、テーブルポイント情報46は、受付部21で受け付けられたコマンド制御情報に基づいて、アドレステーブル23a-2をポイントするための情報で、テーブルポイント情報48は、受付部21で受け付けられたアクセス制御情報に基づいて、アドレステーブル23a-2をポイントするための情報である。ここで、アドレステーブル23a-2には、上述のコマンド空間領域情報45で指定された領域内の位置を、コード化されたコマンド情報をキーとして登録するとともに、アクセス空間領域情報47で指定されたアクセス制御情報の領域を、コード化されたアクセス制御情報をキーとしてアドレス情報により登録するものである。

【0073】すなわち、領域制御部23では、受付部21においてコマンド情報またはアクセス制御情報を受け付けると、これらの情報をキーとして、アドレステーブル23a-2を検索することにより、上述のコマンド情報またはアクセス制御情報に対応するメモリ30上のアドレスを抽出することができるようになっている。とこ

るで、共用空間テーブル23a-1は、上述のID情報41に対応するアプリケーションで使用する他に、他のアプリケーションにおいても共用して用いることができる共用アクセス空間および共用コマンド空間を登録するものであり、認証情報49、コマンド空間領域情報50、テーブルポイント情報51、アクセス空間領域情報52およびテーブルポイント情報53をそなえて構成されている。

【0074】ここで、認証情報49は、後述する共用拡張アドレスを用いた処理を行なう際に必要な上位装置40の使用者の認証情報を照合するためのものであり、この認証情報の照合を通じて、上位装置40の使用者が、メモリ30上の共用拡張アドレス空間にアクセスできる資格を有しているか否かを判定することができる。また、共用コマンド空間領域情報50は、ID情報41に対応するアプリケーションにおけるコマンド空間のうち、他のアプリケーションにおいても使用しうる共用コマンド空間の領域について示すものである。すなわち、この共用コマンド空間領域情報50は、共用コマンド空間を、メモリ30上の開始位置情報と終了位置情報とで設定するものであるが、これら開始位置および終了位置の情報についても、例えばアドレス情報を用いることができる。

【0075】具体的には、通常の共用コマンド情報を記憶するメモリ30上の開始アドレスおよび終了アドレスが登録された共用コマンド空間情報50aをそなえると同時に、拡張された共用コマンド情報を記憶するメモリ30上の領域を、開始アドレスおよび終了アドレスで設定された共用拡張コマンド空間情報50bをそなえている。

【0076】さらに、共用アクセス空間領域情報52は、ID情報41に対応するアプリケーションにおけるアクセス空間の領域のうち、他のアプリケーションにおいても使用しうる共用アクセス空間について示すものである。すなわち、この共用アクセス空間領域情報52は、共用アクセス空間を、メモリ30上の開始位置情報と終了位置情報とで指定するもので、これら開始位置情報および終了位置情報についても、例えばアドレス情報を用いることができる。

【0077】具体的には、共用アクセス空間領域情報52としては、アクセス対象の共用データ領域についてのメモリ30上の開始アドレスおよび終了アドレスで設定する共用データ空間情報52aをそなえると同時に、共用アクセス制御情報をメモリ30上の開始アドレスおよび終了アドレスで設定する共用アクセス制御空間情報52bをそなえている。

【0078】また、テーブルポイント情報51は、受付部21で受け付けられた共用コマンド情報に基づいて、アドレステーブル23a-3をポイントするための情報で、テーブルポイント情報53は、受付部21で受け付

けられた共用アクセス制御情報に基づいて、アドレステーブル23a-3をポイントするための情報である。ここで、アドレステーブル23a-3には、コード化されたコマンド情報およびアクセス制御情報に対応したメモリ30上の位置を、アドレス情報で登録するものであるが、コード化されたコマンド情報に対応したメモリ30上の位置は、上述の共用コマンド空間領域情報50で指定された領域内に存在し、コード化されたアクセス制御情報に対応したメモリ30上の位置は、アクセス空間領域情報47で指定された領域内に存在する。

【0079】すなわち、領域制御部23では、受付部21において共用コマンド情報または共用アクセス制御情報を受け付けると、これらの情報をキーとして、アドレステーブル23a-2を検索することにより、対応するメモリ30上のアドレスを抽出することができるようになっている。なお、上述の空間テーブル23aにおいては、各空間32、33をメモリ30上の領域における開始位置情報と終了位置情報で指定しているが、この領域指定で用いられる位置情報は、上述のごときアドレス情報のほか、例えば図6に示すようなビット表現されたページ情報とすることもできる。この場合においては、ページ情報をアドレス情報に変換するための図示しないテーブルを用いることにより、メモリ30へのアクセスを行なうこともできる。

【0080】換言すれば、領域制御部23において領域テーブル23aを参照することにより、受付部21にて受け付けられたアプリケーション処理依頼に対応した処理を実行するためのメモリ30上の領域を、アドレス情報またはページ情報により抽出することができるのである。すなわち、領域制御部23を、受付部21にて受け付けられたアプリケーション処理依頼に対応した処理を実行するための上記メモリ上の領域を、空間テーブル23aを参照することにより、ページ情報により抽出できるようにすれば、例えば不連続にメモリ領域を使用することができる。

【0081】ところで、上述の領域監視部24は、領域制御部23にて抽出された領域設定情報を登録しておくコントロールレジスタ24aをそなえて構成され、命令実行部21にてメモリアクセスが発生したアドレスが、コントロールレジスタ24aにてハードウェア的に設定された領域情報内のアドレス（あるいはページ）か否かを判定するようになっているが、このコントロールレジスタ24aには、詳細には例えば図7に示すような情報が設定されるようになっている。

【0082】すなわち、このコントロールレジスタ24aには、領域制御部23における空間テーブル23aの検索結果に基づいて設定する情報に応じて、空間モード設定部54、ステータス設定部55、共用空間領域設定部56および空間領域設定部57が設けられている。ここで、空間モード設定部54は、受付部22にて受け付

10

20

30

40

50

けられたアプリケーション処理依頼に基づいて、CPU 20としての命令実行部21において動作状態となる空間識別子を設定するものであり、命令実行部21がOS空間31で動作する場合には、“O”が設定され、アクセス空間32で動作する場合には、“A”が設定され、コマンド空間33で動作する場合には、“C”が設定される。

【0083】また、ステータス登録部55は、上述の空間テーブル23aによりアクセス空間32およびコマンド空間33を指定する方式の識別情報を設定するとともに、受付部22にて受け付けられたアプリケーション処理依頼がコマンド情報である場合に、当該コマンドの種別を示す情報について設定するものである。具体的には、前述の図8に示すアクセス空間32およびコマンド空間33をアドレスにより指定する場合には種別情報として“AD”を、ページ情報で指定する場合には“PG”を、それぞれ設定する。また、受け付けたコマンド情報が通常のコマンドである場合には種別情報として“N”を、コマンド情報が通常の拡張コマンドである場合には種別情報として“E”を、コマンド情報が共用拡張コマンドである場合には種別情報として“K”を、それぞれ設定する。

【0084】さらに、共用空間領域設定部56は、受付部22にて受け付けられたアプリケーションの種別に応じて、他のアプリケーションと共用しうる共用アクセス空間や共用コマンド空間に属する領域情報について設定するものである。例えば、図8に示すように空間が設定された場合は、共用空間領域設定部56では、他のアプリケーションと共用のデータ（共用データ）、アクセス制御情報（共用アクセス制御情報）が記憶されたメモリ30上の領域32B-3、32C-3とともに、コマンド（共用コマンド情報）あるいは拡張コマンド（共用拡張コマンド）が記憶されたメモリ30上の領域33C-3、33C-31の領域情報について設定されることになる。

【0085】空間領域設定部57は、受付部22にて受け付けられたアプリケーションの種別（例えば電子マネーのアプリケーション）に応じて、他のアプリケーションと共用しないアクセス空間やコマンド空間に属する領域情報について設定するものである。すなわち、上述の図8に示すように空間が設定された場合は、空間領域情報設定部57では、他のアプリケーション（例えば医療情報アプリケーション）と共用しないデータおよびアクセス制御情報が記憶されたメモリ30上の領域32B-1、32C-2とともに、コマンド情報あるいは拡張コマンドが記憶されたメモリ30上の領域33C-1、33C-11に關しての領域情報が設定されることになる。

【0086】したがって、上述の領域監視部24のコントロールレジスタ24aにより、領域制御部23にて抽

出されたメモリ30上の領域を登録しておき、登録された情報に基づいて、命令実行部21における処理が実行されているか否かを監視することができるのである。

(E) 本実施形態にかかるICカードの発行処理の説明
本実施形態にかかるICカード10は、図15に示すようなライフサイクルを有している。すなわち、この図15に示すICカード10は、ICチップをカード内に埋め込むことを通じて製造され（ステップS1）、さらに、カード発行装置（図3の符号15、16参照）において所望のアプリケーションのためのソフトウェアのローディング処理や、使用者が持つ認証情報を登録すること等を通じて発行する（ステップS2）。

【0087】その後、ICカード10は使用者により運用され（ステップS3）、最終的に償却されることとなるが（ステップS4）、当該使用者の必要性に応じて、適宜他のアプリケーションのためのソフトウェアをカード発行装置にてローディングすることにより、特に複数のアプリケーション処理を実現するための機能を有するICカードとして再発行を行なうことができる（ステップS2からステップS3）。

【0088】ところで、上述のカード発行の際には、ICカード10内のプログラムのセキュリティを確保すべく、使用者がICカード10および上位装置40を操作しうる本人であるか否かを認証することが要求される。この本人の認証を行なう手法としては、例えば図16または図17に示すようなものがある。すなわち、図16に示す本人の認証を行なう手法としては、カード発行装置としての上位装置40Aから通知された認証情報と、ICカード10とは別に使用者が所持する本人認証カード60にて保有される本人認証情報とを照合し、一致する（照合が成功した）認証情報があれば当該一致した認証情報とともに認証結果を上位装置40Aに通知するものである。

【0089】換言すれば、ICカード10を発行しうる上位装置40A固有の認証情報を、認証情報を予め記憶する外部カード媒体としての本人認証カード60に通知し（認証情報通知ステップ）、本人認証カード60において、上位装置40Aからの認証情報と、当該本人認証カード60にて記憶される認証情報とを照合、認証し、上位装置40Aを介してICカード10の発行可否を判定する（照合判定ステップ）。上述の判定の結果、ICカード10を発行可と判定された場合に、上位装置40Aを介して所望のICカード10を発行し（発行ステップ）、発行されたICカード10を用いて上位装置40Aから依頼された所望のアプリケーション処理を実行することができる。

【0090】具体的には、本人認証カード60では、上位装置40Aからのステータス情報61として記憶される認証データの種別を示すデータ種情報（D）と、認証データ62とを用いて照合を行なうことができるほか、

ステータス情報61として記憶される受信時間情報

(T)と認証データ62とを用いて照合を行なうことができる。

【0091】これにより、本人認証カード60にて認証が成功した（一致する認証情報を検出した）場合には、上位装置40Aにおいてカード発行の際の認証情報を空間テーブル23aに設定することにより、この上位装置40Aを介してICカード10を発行することができるのである。なお、上位装置40Aから送信されるステータス情報61を構成するデータ種において、“NO”は10 認証データ62がデータ無しの場合を示し、“PN”は認証データ62が暗証番号の場合を示し、“SI”は認証データ62が本人のサインの場合を示し、“PH”は認証データ62が写真データの場合を示し、“FI”は認証データ62が指紋データの場合を示し、“RE”は認証データ62が虹彩データの場合を示し、“VO”は認証データ62が声紋データの場合を示している。

【0092】この場合においては、本人認証カード60では、上位装置40Aから通知されない「網膜データ」では、照合は成功しないことになる。また、集積回路が埋め込まれた（アプリケーション処理用のプログラムが記憶されていない）カードのプログラムデータをローディングし、ICカード10として発行する際には、これに先立って、例えば図17に示すような認証情報の照合が行なわれる。

【0093】すなわち、図17に示すように、本人認証カード60の認証情報をICカード10に通知するとともに、ICカード10の認証情報を本人認証カード60に対して通知し（認証情報通知ステップ）、本人認証カード60において、ICカード10から通知された認証10 情報と本人認証カード60にて記憶される認証情報とを照合、認証するとともに、ICカード10において、本人認証カード60から通知された認証情報とICカード10にて記憶される認証情報とを照合、認証することにより、上位装置40Aを介しての上記プログラムデータの書き込み可否を判定し（照合判定ステップ）、この判定の結果上記プログラムデータが書き込み可と判定された場合に、ICカード10では、上位装置40Aを介して書き込み処理を実行することを通じ（書込処理実行ステップ）、書き込みの際の本人の認証を行なうこともできる。

【0094】具体的には、発行されたICカード10の空間テーブル23aに予め設定された認証情報と、本人認証カード60からの認証情報とを相互に照合し（ICカード10および本人認証カード60の双方で照合し）、双方のカード10、60にて認証が成功した場合に、当該ICカード10について再発行処理等を行なう。ここで、本人認証カード60は、この図17に示すように、利用しうるアプリケーション毎に、当該アプリケーションを識別するための情報（AID）63、IC

カード10における空間テーブル23a、共用空間テーブル23a-1で使用される認証情報64、65とを登録する認証情報テーブル66をそなえている。

【0095】これにより、本人認証カード60では、ICカード10の製造時に予め設定された認証情報を、ICカード10から上位装置40Aを介して入力され、この認証情報と上述の認証情報テーブル66にて登録される認証情報64とを照合する。さらに、ICカード10では、本人認証カード60における認証情報テーブル66にて登録される認証情報64を、本人認証カード60から上位装置40Aを介して入力され、この認証情報64とICカード10の製造時に予め設定された認証情報とを照合する。

【0096】したがって、上述のICカード10および本人認証カード60において相互に認証情報を照合し

（①参照）、上位装置40Aにおいて、上述のICカード10および本人認証カード60の双方において照合結果が一致した場合に、空間テーブル23aを設定した後に、プログラムデータをローディングし、アドレステーブル23a-1、23a-3を設定することができる

（②参照）。

【0097】ところで、上述の空間テーブル23aをICカード10に設定する際に、例えば図18に示すように、照合された認証情報に応じてプロテクションフラグ領域35をOS空間31に設定し、その後に、プログラムデータをICカード10にローディングすることができるようになっている。ここで、このプロテクションフラグ領域34は、特定の認証情報を所持しない使用者による特定のアプリケーション処理を禁止するためのフラグ情報を記憶するもので、このプロテクションフラグ領域34としては、メモリ30上の特定の領域部分に、当該領域部分の読み出しおよび書き込みを禁止するビット情報としてのプロテクションフラグ35をページ対応に設定する。

【0098】すなわち、上述のアクセス空間32またはコマンド空間33からの、特定のアプリケーション処理を行なうためのメモリ30の領域に対するページ単位のアクセスを、OS空間31において禁止することができるようになっている。例えば、プログラム開発者以外の使用者が書き込みできない領域をプロテクションフラグ領域34で設定しておくことにより、プログラムの改ざんや、認証情報を照合するための暗号アルゴリズムやキー若しくは暗号処理の改ざんを防止することができる。

【0099】ここで、この図18におけるメモリ30上の「8000番地」のページには、使用者からの書き込みを禁止すべき情報として、例えば領域制御部23としての機能を実現するためのプログラムデータが記憶されており、当該「8000番地」にはプロテクションフラグ34としてのビット情報“1”が設定され、「8010番地」や「8020番地」のページ等、メモリ30上

の空き領域には書き込み可能なフラグ34としてのビット情報“0”が設定されている。

【0100】なお、ICカード10にローディングするプログラムとしては、認証が行なわれた本人認証カード60から上位装置40Aを介して直接ローディングしてもよく（本人認証カード60に予め記憶されたプログラムデータをローディングしてもよく）、また、別媒体に記憶されたプログラムデータについて、上位装置40Aを介してローディングすることもできる。

【0101】また、上述のICカード10側で製造時に予め記憶された空間テーブル23aの認証情報44の他に、ICカード10を発行する上位装置40Aにて予め記憶されている認証情報を用いることにより、上位装置40Aおよび本人認証カード60において相互に認証を行なうようにしてもよい。

（F）本実施形態にかかるICカード利用による作用効果の説明

上述の構成により、本実施形態にかかるICカード10を利用する際の動作について、図19～図22を用いて以下に説明する。

【0102】（F1）アクセス空間とコマンド空間との間の切替動作の一例の説明

ICカード10においては、上位装置40からアプリケーション処理依頼に関するコマンドを受けける場合には、当該上位装置40から、依頼されたアプリケーション処理を識別するための情報（AID）のほか、コマンド情報を構成するコード情報やパラメータ情報等をOS空間31にて受け付ける。

【0103】OS空間31においては、例えば図19に示すように、この上位装置40からのコマンド処理を実行すべく、必要に応じて実行状態をアクセス空間72またはコマンド空間73に遷移させるように制御する。すなわち、ICカード10のメモリ空間を管理する際に、メモリ30の領域に対応して、アプリケーションが使用するデータを記憶するとともに上記プログラムにおけるアクセス制御が動作するアクセス空間72と、プログラムにおけるアクセス制御以外の処理を行なうためのコマンドが動作するコマンド空間73と、上記のアクセス空間およびコマンド空間における処理を統括制御するOS空間31とを設定し、OS空間31において上位装置40からの処理依頼を受けると、命令実行部21にて処理依頼を実行すべく、OS空間31からアクセス空間72またはコマンド空間73に動作を移行させる。

【0104】具体的には、受付部22において、上位装置40からのコマンド情報（または命令情報）を入力されると（〔1〕参照）、コントロールレジスタ24aの状態をOS空間31に設定するとともに、図示しない通信機構を介してメッセージ（コマンド情報）を組み立てる。続いて、領域制御部23では、上述の受付部22から、コマンドに関してのコード情報（コマンドコード）

およびアプリケーション識別用の情報（AID）を入力されて（〔2〕参照）、当該AIDに基づいて、空間テーブル23aを参照することにより、AIDに対応する空間テーブル23a上の領域に設定されている必要情報を、コントロールレジスタ24aに設定するとともに（〔3〕参照）、上述のコマンド情報に対応するメモリ30上の領域を抽出して、当該処理を命令実行部21に依頼する（〔4〕参照）。

【0105】具体的には、領域制御部23において、受付部22からのAIDにて示されるアプリケーション処理依頼の種別に基づき、対応した処理を実行するためのメモリ30上の領域をアドレステーブル23a-2から抽出する。なお、書き込みおよび読み出しが禁止されている領域のアドレス情報には、プロテクションフラグ35（図18参照）が付されている。

【0106】領域制御部23では、制御がOS空間31からコマンド空間73に移行する際に、命令実行部21に対する処理の依頼に先立って、コントロールレジスタ24aの空間モード情報54をOS空間“O”から、コマンド空間“C”に設定するとともに、空間領域情報57をコマンド空間73（番地「2000」～「2FFF」）に設定するのである（図7参照）。

【0107】命令実行部21では、領域制御部23からの依頼をメモリ30の領域指定により受けて、この抽出されたメモリ30上の領域にアクセスすることにより上述のコマンド情報に対する処理を行なう。これにより、制御はOS空間31からコマンド空間73に移行する（〔4'〕参照）。例えば、ICカード10において、上位装置40から電子マネーアプリケーションにかかるコマンド処理依頼を受けた場合には、命令実行部21では、受け付けられたコマンド処理に対応して、メモリ30上の領域としての番地「2000」に記憶されたプログラム情報を実行する。

【0108】上述したように、命令実行部21では、領域制御部23からメモリ30上の領域指定により依頼されたコマンド処理要求を受けて、対応するメモリ30上の領域にアクセスすることを通じて実行処理が行なわれるが、このとき、領域制御部23にて抽出されたアドレス情報にページ対応のプロテクションフラグ35が付されているか否かを検知し、命令実行可否を制御している。

【0109】領域監視部24では、コントロールレジスタ24aの空間領域57に設定されたコマンド空間73（番地「2000」～「2FFF」）、図8における符号33C-1参照）に基づき、実行処理中の命令処理部21のアクセス先のアドレスが、上述のコマンド空間73内のものか否かを監視している（〔5〕、〔6〕参照）。

【0110】さらに、命令処理部21において、上述のコマンド処理を実行中にアクセス空間72（番地「40

00～4FFF」，図8における符号32B-1，32C-1参照)に対するアクセス要求が発生した場合には、OS空間31内で動作する受付部22に当該アクセス要求が通知される(〔7〕参照)。受付部22においては、アクセス空間72に対するアクセス要求(空間切替命令)を入力されると、コントロールレジスタ24aの状態をOS空間31に設定するとともに、当該空間切替命令を示す命令コードを捕捉(キャッチ)する。

【0111】続いて、領域制御部23では、上述の受付部22から空間切替命令のコード情報を入力され

(〔8〕参照)、当該空間切替命令に対応するアドレス情報を、空間テーブル23aにポイントされたアドレステーブル23a-2から検索、抽出する。なお、書き込みおよび読み出しが禁止されている領域のアドレス情報には、プロテクションフラグ35(図18参照)が付されている。

【0112】これにより、領域制御部23では、空間テーブル23aに設定されている必要情報を、コントロールレジスタ24aに設定するとともに(〔9〕参照)、命令実行部21に対して該当するアドレス情報による処理の実行を依頼する(〔10〕参照)。

【0113】具体的には、領域制御部23において、受付部22からの空間切替命令に基づき、対応した処理を実行するためのメモリ30上の領域をアドレステーブル23a-2から抽出する。命令実行部21においては、領域制御部23からの依頼をメモリ30の領域指定により受けて、この抽出されたメモリ30上の領域にアクセスすることにより上述の空間切替情報に対する処理を行なう。これにより、制御はOS空間31からアクセス空間72に移行する(〔10′〕参照)。

【0114】すなわち、領域制御部23では、制御がOS空間31からアクセス空間72に移行する際に、命令実行部21に対する処理の依頼に先立って、コントロールレジスタ24aの空間モード情報54，ステータス情報55および空間領域情報57を設定する。具体的には、空間モード情報54をアクセス空間72を示す

“A”に設定し、ステータス情報55のコマンドステータスを無設定(“-”)とするとともにメモリ30指定方式をアドレス指定“AD”と設定し、空間領域情報57をアクセス空間72(番地「4000」～「4FFF」)に設定するのである。

【0115】例えば、上述の電子マネーアプリケーションに適用されたICカード10のOS空間31において、コマンド空間73による処理中にアクセス空間72への空間切替を行なうことにより、例えばメモリ30上の領域としての番地「4000」に記憶されたプログラム情報を実行する。上述したように、命令実行部21では、領域制御部23からメモリ30上の領域指定により依頼されたコマンド処理要求を受けて、対応するメモリ30上の領域にアクセスすることを通じて実行処理が行

なわれるが、このとき、ページ対応のプロテクションフラグ35の有無を検知し、命令実行可否を制御している。

【0116】また、領域監視部24では、コントロールレジスタ24aの空間領域57に設定されたアクセス空間72(番地「4000」～「4FFF」，図8における符号32B-1参照)に基づき、実行処理中の命令処理部21のアクセス先のアドレスが、上述のコマンド空間73内のものか否かを監視している(〔11〕，〔12〕参照)。

【0117】(F2)アクセス空間とコマンド空間との間の切替動作の一例の説明

ICカード10においては、上位装置40から電子マネーアプリケーションの処理依頼に関するコマンドを受けると、上述の場合と同様に、命令処理部21においてコマンド空間73(図8における符号33C-1参照)における処理が行なわれる(図20の〔1〕～〔6〕，

〔4′〕参照)。なお、この図20における処理ステップ〔1〕～〔6〕，〔4′〕は、図19に示す処理ステップ〔1〕～〔6〕，〔4′〕に対応している。

【0118】ここで、上述の命令実行部21において、コマンド処理を実行中に、コマンド空間73を、拡張コマンド空間73A(番地「3000～3FFF」，図8における符号33C-1参照)に拡張する旨の要求(領域拡張要求)が発生した場合には、OS空間31内で動作する受付部22に当該領域拡張要求が通知される(〔7〕参照)。

【0119】受付部22においては、拡張コマンド空間73Aに対するアクセス要求(領域拡張命令)を入力されると、コントロールレジスタ24aの状態をOS空間31に設定するとともに、当該領域拡張命令を示す命令コードを捕捉(キャッチ)する。続いて、領域制御部23では、上述の受付部22から領域拡張命令のコード情報を入力され(〔8〕参照)、当該領域拡張命令に対応するアドレス情報を、空間テーブル23aにポイントされたアドレステーブル23a-2から検索、抽出する。なお、書き込みおよび読み出しが禁止されている領域のアドレス情報には、プロテクションフラグ35(図18参照)が付されている。

【0120】これにより、領域制御部23では、空間テーブル23aに設定されている必要情報を、コントロールレジスタ24aに設定するとともに(〔9〕参照)、命令実行部21に対して該当するアドレス情報による処理の実行を依頼する(〔10〕参照)。具体的には、領域制御部23において、受付部22からの領域拡張命令に基づき、対応した処理を実行するためのメモリ30上の領域をアドレステーブル23a-2から抽出する。命令実行部21においては、領域制御部23からの依頼をメモリ30上の領域指定により受けて、この抽出されたメモリ30上の領域にアクセスすることにより上述の領域

10

20

30

40

50

拡張情報に対する処理を行なう。これにより、制御はOS空間31から拡張コマンド空間73Aに移行する（〔10'〕参照）。

【0121】なお、領域制御部23では、制御がOS空間31から拡張コマンド空間73Aに移行する際に、命令実行部21に対する処理の依頼に先立って、コントロールレジスタ24aの空間モード情報54、ステータス情報55および空間領域情報57を設定する。具体的には、空間モード情報54をコマンド空間“A”に設定し、ステータス情報55のコマンドステータスを拡張コマンド“E”に設定するとともにメモリ30の領域の指定方式をアドレス指定“AD”と設定し、空間領域情報57を拡張コマンド空間73A（番地「2000」～「3FFF」）に設定するのである。

【0122】なお、命令実行部21では、領域制御部23からメモリ30上の領域指定により依頼された拡張コマンド処理要求を受けて、対応するメモリ30上の領域にアクセスすることを通じて実行処理が行なわれるが、このとき、ページ対応のプロテクションフラグ35の有無を検知し、命令実行可否を制御している。また、領域監視部24では、コントロールレジスタ24aの空間領域57に設定された拡張コマンド空間73A（番地「2000」～「3FFF」）、図8における符号33C-1（参照）に基づき、実行処理中の命令処理部21のアクセス先のアドレスが、上述の拡張コマンド空間73A内のものか否かを監視している（〔11〕、〔12〕参照）。

【0123】（F3）共用アクセス空間と共用コマンド空間との間の切替動作の一例の説明

ICカード10においては、例えば図21に示すように、上位装置40からの電子マネーアプリケーションの処理依頼に関するコマンドのうちで、共用コマンド空間73B（図8における符号33C-3参照）に該当するコマンドについては、当該共用コマンド空間73Bにおいて処理が行なわれる。

【0124】具体的には、受付部22において、上位装置40からのコマンド情報（または命令情報）を入力されると（〔1〕参照）、コントロールレジスタ24aの状態をOS空間31に設定するとともに、図示しない通信機構を介してメッセージ（コマンド情報）を組み立てる。続いて、領域制御部23では、上述の受付部22から、コマンドに関してのコード情報（コマンドコード）およびアプリケーション識別用の情報（AID）を入力されて（〔2〕参照）、当該AIDに基づいて、空間テーブル23aを参照することにより、AIDに対応する空間テーブル23a上の領域に設定されている必要情報を、コントロールレジスタ24aに設定するとともに（〔3〕参照）、上述のコマンド情報に対応するメモリ30上の領域を抽出して、当該処理を命令実行部21に依頼する（〔4〕参照）。

【0125】具体的には、領域制御部23において、受付部22からのコマンド情報に基づき、空間テーブル23aにポイントされたアドレステーブル23a-2を参照することにより、対応した処理を実行するためのメモリ30上の領域として、他のアプリケーション処理におけるコマンド処理の際に共通に用いられる共用コマンド空間73B（例えば番地「2000」～「2FFF」）を抽出する。なお、書き込みおよび読み出しが禁止されている領域のアドレス情報には、プロテクションフラグ35（図18参照）が付されている。

【0126】命令実行部21では、領域制御部23からの依頼をメモリ30の領域指定により受けて、指定されたメモリ30上の領域にアクセスすることにより上述のコマンド情報に対する処理を行なう。これにより、制御はOS空間31からコマンド空間73に移行する（〔4'〕参照）。なお、領域制御部23では、制御がOS空間31から共用コマンド空間73に移行する際に、命令実行部21に対する処理の依頼に先立って、コントロールレジスタ24aの空間モード情報54、ステータス情報55および共用空間領域56を設定するのである（図7参照）。

【0127】具体的には、空間モード情報54をコマンド空間“C”に設定し、ステータス情報55のコマンドステータスを通常コマンド“N”に設定するとともにメモリ30の領域の指定方式をアドレス指定“AD”と設定し、共用空間領域情報56を共用コマンド空間73B（番地「2000」～「3FFF」）に設定するのである。

【0128】上述したように、命令実行部21では、領域制御部23からメモリ30上の領域指定により依頼されたコマンド処理要求を受けて、対応するメモリ30上の領域にアクセスすることを通じて実行処理が行なわれるが、このとき、領域制御部23にて抽出されたアドレス情報にページ対応のプロテクションフラグ35が付されているか否かを検知し、命令実行可否を制御している。

【0129】領域監視部24では、コントロールレジスタ24aの空間領域57に設定された共用コマンド空間73B（番地「2000」～「2FFF」）、図8における符号33C-3参照）に基づき、実行処理中の命令処理部21のアクセス先のアドレスが、上述のコマンド空間73内のものか否かを監視している（〔5〕、〔6〕参照）。

【0130】さらに、命令処理部21において、上述のコマンド処理を実行中に共用アクセス空間72C（番地「4000～4FFF」）、図8における符号32B-3、32C-3参照）に対するアクセス要求が発生した場合には、OS空間31内で動作する受付部22に当該アクセス要求が通知される（〔7〕参照）。受付部22においては、共用アクセス空間72Bに対するアクセス

要求(空間切替命令)を入力されると、コントロールレジスタ24aの状態をOS空間31に設定するとともに、当該空間切替命令を示す命令コードを捕捉(キャッチ)する。

【0131】続いて、領域制御部23では、上述の受付部22から空間切替命令のコード情報を入力され

(〔8〕参照)、当該空間切替命令に対応するアドレス情報を、空間テーブル23aにポイントされた共用アドレステーブル23a-3から検索、抽出する。なお、書き込みおよび読み出しが禁止されている領域のアドレス情報には、プロテクションフラグ35(図18参照)が付されている。

【0132】これにより、領域制御部23では、空間テーブル23aに設定されている必要情報を、コントロールレジスタ24aに設定するとともに(〔9〕参照)、命令実行部21に対して該当するアドレス情報による処理の実行を依頼する(〔10〕参照)。具体的には、領域制御部23において、受付部22からの空間切替命令に基づき、対応した処理を実行するためのメモリ30上の領域をアドレステーブル23a-2から抽出する。命令実行部21においては、領域制御部23からの依頼をメモリ30の領域指定により受けて、この抽出されたメモリ30上の領域にアクセスすることにより上述の空間切替情報に対する処理を行なう。これにより、制御はOS空間31から共用アクセス空間72Bに移行する(〔10'〕参照)。

【0133】すなわち、領域制御部23では、制御がOS空間31から共用アクセス空間72Bに移行する際に、命令実行部21に対する処理の依頼に先立って、コントロールレジスタ24aの空間モード情報54、ステータス情報55および空間領域情報57を設定する。具体的には、空間モード情報54を共用アクセス空間72Bを示す“A”に設定し、ステータス情報55のコマンドステータスを無設定(“-”)とするとともにメモリ30指定方式をアドレス指定“AD”と設定し、共用空間領域情報56を共用アクセス空間72B(番地「4000」~「4FFF」)に設定するのである。

【0134】例えば、上述の電子マネーアプリケーションに適用されたICカード10のOS空間31において、共用コマンド空間73Bによる処理中に共用アクセス空間72Bへの空間切替を行なうことにより、例えばメモリ30上の領域としての番地「4000」に記憶されたプログラム情報を実行する。上述したように、命令実行部21では、領域制御部23からメモリ30上の領域指定により依頼されたコマンド処理要求を受けて、対応するメモリ30上の領域にアクセスすることを通じて実行処理が行なわれるが、このとき、ページ対応のプロテクションフラグ35の有無を検知し、命令実行可否を制御している。

【0135】また、領域監視部24では、コントロール

レジスタ24aの共用空間領域情報56に設定された共用アクセス空間72B(番地「4000」~「4FFF」, 図8における符号32B-3, 32C-3参照)に基づき、実行処理中の命令処理部21のアクセス先のアドレスが、上述の共用アクセス空間72B内のものか否かを監視している(〔11〕, 〔12〕参照)。

【0136】(F4)アクセス空間とコマンド空間との間の切替動作の一例の説明

ICカード10においては、例えば図22に示すように、上位装置40からの電子マネーアプリケーションの処理依頼が、共用コマンド空間73B(図8における符号33C-3参照)に該当するコマンドである場合については、上述の場合(図20参照)と同様に、命令処理部21において共用コマンド空間73B(図8における符号33C-3参照)における処理が行なわれる(図22の〔1〕~〔6〕, 〔4'〕参照)。なお、この図22における処理ステップ〔1〕~〔6〕, 〔4'〕は、図21に示す処理ステップ〔1〕~〔6〕, 〔4'〕に対応している。

【0137】ここで、上述の命令実行部21において、コマンド処理を実行中に、共用コマンド空間73B(番地「2000~2FFF」, 図8における符号33C-3参照)を、共用拡張コマンド空間73C(番地「2000~3FFF」, 図8における符号33C-31参照)に拡張する旨の要求(領域拡張要求)が発生した場合には、OS空間31内で動作する受付部22に当該領域拡張要求が通知される(〔7〕参照)。

【0138】受付部22においては、共用拡張コマンド空間73Cに対するアクセス要求(領域拡張命令)を入力されると、コントロールレジスタ24aの状態をOS空間31に設定するとともに、当該領域拡張命令を示す命令コードを捕捉(キャッチ)する。続いて、領域制御部23では、上述の受付部22から領域拡張命令のコード情報を入力され(〔8〕参照)、当該領域拡張命令に対応するアドレス情報を、空間テーブル23aにポイントされた共用アドレステーブル23a-3から検索、抽出する。なお、書き込みおよび読み出しが禁止されている領域のアドレス情報には、プロテクションフラグ35(図18参照)が付されている。

【0139】これにより、領域制御部23では、空間テーブル23aに設定されている必要情報を、コントロールレジスタ24aに設定するとともに(〔9〕参照)、命令実行部21に対して該当するアドレス情報による処理の実行を依頼する(〔10〕参照)。具体的には、領域制御部23において、受付部22からの領域拡張命令に基づき、対応した処理を実行するためのメモリ30上の領域を共用アドレステーブル23a-3から抽出する。命令実行部21においては、領域制御部23からの依頼をメモリ30の領域指定により受けて、この抽出されたメモリ30上の領域にアクセスすることにより上述

の領域拡張情報に対する処理を行なう。これにより、制御はOS空間31から共用拡張コマンド空間73Cに移行する（〔10'〕参照）。

【0140】すなわち、領域制御部23では、制御がOS空間31から共用拡張コマンド空間73Cに移行する際に、命令実行部21に対する処理の依頼に先立って、コントロールレジスタ24aの空間モード情報54、ステータス情報55および共用空間領域情報56を設定する。具体的には、空間モード情報54をコマンド空間“A”に設定し、ステータス情報55のコマンドステータスを共用拡張コマンド“K”に設定するとともにメモリ30の領域の指定方式をアドレス指定“AD”と設定し、共用空間領域情報56を共用拡張コマンド空間73C（番地「2000」～「3FFF」）に設定するのである。

【0141】なお、命令実行部21では、領域制御部23からメモリ30上の領域指定により依頼された拡張コマンド処理要求を受けて、対応するメモリ30上の領域にアクセスすることを通じて実行処理が行なわれるが、このとき、ページ対応のプロテクションフラグ35の有無を検知し、命令実行可否を制御している。また、領域監視部24では、コントロールレジスタ24aの空間領域56に設定された共用拡張コマンド空間73C（番地「2000」～「3FFF」）、図8における符号33C-31参照）に基づき、実行処理中の命令処理部21のアクセス先のアドレスが、上述の共用拡張コマンド空間73C内のものか否かを監視している（〔11〕、〔12〕参照）。

【0142】このように、本実施形態によれば、受付部21と、領域制御部23と、領域監視部24とをそなえ、メモリ30の領域に対応して、アクセス制御が動作するアクセス空間72と、コマンドが動作するコマンド空間73と、上記のアクセス空間72およびコマンド空間73における処理を統括制御するOS空間31とを設定し、OS空間31において上位装置40からの処理依頼を受けると、命令実行部21にて処理依頼を実行すべく、OS空間31から上記のアクセス空間72またはコマンド空間73に動作を移行させることができるので、記憶されているデータのセキュリティ機能を保全すべく、アプリケーション機能を実現するプログラムを動作させる際に、CPU20の動作領域を予めメモリ30上に制限的に設定しておくことにより、他のアプリケーション機能によって管理されるデータを取り出すことを防止することができ、ひいては、各アプリケーション各自が持つ暗号アルゴリズム／キー／暗号処理を、他アプリケーションを介して改ざんすることを防護できる。

【0143】例えば、電子マネーアプリケーションで管理されるデータを、医療情報のアプリケーションからの取り出しを防止することを通じ、使用者により任意にアプリケーションをローディングする場合においても、各

アプリケーションにて管理されるデータを保全することができるのである。さらに、コマンド空間73の動作中における該統括制御空間に対する宣言に基づいて、コマンド空間73を拡張させることができるので、例えば認証情報の照合の際に、プログラム開発者と認証された使用者以外の使用者が書き込みできない領域をブラックボックスとしての拡張領域として設定しておけば、同一アプリケーションの一部で機密処理（ブラックボックス）することも可能であり、プログラムの改ざんや、認証情報を照合するための暗号アルゴリズムやキー若しくは暗号処理の改ざんを防止することができる。

【0144】また、アプリケーション毎に分割して設定されるアクセス空間72や、コマンドが実行できるコマンド空間73一部を、相互に共用化された空間とすることができるので、アクセス空間72およびコマンド空間73での空間共用制御を実現することができ、メモリ領域を有効に利用することができる利点がある。さらに、認証情報通知ステップと、照合判定ステップと、発行ステップ（または書込処理実行ステップ）により、ICカード10を発行することで、ICチップ／ICカードの製造時に認証情報を設定するため、製造からICカード10の発行までの間で媒体の改ざん等を防止することができるほか、本人認証カード60を基にした認証を行なうため、重要なプログラム書き込み処理（例えば、空間テーブル23aにおけるAID41に関連する空間領域56、57の定義や空間メモリダンプ処理等）を、アプリケーション管理者等のみが行なうことができる利点もある。

【0145】なお、上述の本実施形態においては、ICカードについて本発明を適用した場合について詳述したが、これに限定されず、ICカード以外の何らかの可搬型カード媒体に本発明を適用してもよい。

【0146】

【発明の効果】以上詳述したように、本発明（請求項1～17）によれば、受付機構と、領域制御機構と、領域監視機構とをそなえ、メモリの領域に対応して、アクセス制御が動作するアクセス空間と、コマンドが動作するコマンド空間と、上記のアクセス空間およびコマンド空間における処理を統括制御する統括制御空間とを設定し、統括制御空間において上位装置からの処理依頼を受けると、実行処理機構にて処理依頼を実行すべく、統括制御空間から上記のアクセス空間またはコマンド空間に動作を移行させることができるので、記憶されているデータのセキュリティ機能を保全すべく、アプリケーション機能を実現するプログラムを動作させる際に、実行処理機構の動作領域を予めメモリ上に制限的に設定しておくことにより、他のアプリケーション機能によって管理されるデータを取り出すことを防止することができ、ひいては、他アプリケーションを介して、各アプリケーション各自が持つ暗号アルゴリズム／キー／暗号処理が改

ざんされることを防護することができる。

【0147】さらに、請求項14記載の本発明によれば、コマンド空間の動作中における該統括制御空間に対する宣言に基づいて、コマンド空間を拡張させることができるので、例えば認証情報の照合の際に、プログラム開発者と認証された使用者以外の使用者が書き込みできない領域をブラックボックスとしての拡張領域として設定しておけば、同一アプリケーションの一部で機密処理（ブラックボックス）することも可能であり、プログラムの改ざんや、認証情報を照合するための暗号アルゴリズムやキー若しくは暗号処理の改ざんを防止することができる。

【0148】また、請求項11、13記載の本発明によれば、アプリケーション毎に分割して設定されるアクセス空間や、コマンドが実行できるコマンド空間の一部を、相互に共用化された空間とすることができるので、アクセス空間およびコマンド空間での空間共用制御を実現することができ、メモリ領域を有効に利用することができる利点がある。

【0149】さらに、請求項15、16記載の本発明によれば、認証情報通知ステップと、照合判定ステップと、発行ステップ（書込処理実行ステップ）とをそなえたことにより、可搬型カード媒体の製造時に認証情報を設定するため、製造からカードの発行までの間で媒体の改ざん等を防止することができるほか、外部装置を基にした認証を行なうため、重要なプログラム書き込み処理等を、アプリケーション管理者等のみが行なうことができる利点もある。

【図面の簡単な説明】

【図1】本発明の原理ブロック図である。

【図2】本発明の一実施形態にかかるICカードを示すブロック図である。

【図3】本実施形態にかかる各種アプリケーションシステムを実現するICカードの上位装置への接続態様を示す図である。

【図4】本実施形態における各アプリケーションのプログラムやデータが記憶される領域を説明するための図である。

【図5】本実施形態における領域制御部にて参照される空間テーブルを示す図である。

【図6】本実施形態における領域制御部にて参照される空間テーブルの要部を示す図である。

【図7】本実施形態における領域監視部のコントロールレジスタに設定される情報を示す図である。

【図8】本実施形態におけるCPU20の動作領域としてのOS空間、アクセス空間およびコマンド空間を示す図である。

【図9】本実施形態におけるCPU20の動作領域としてのOS空間、アクセス空間およびコマンド空間を示す図である。

【図10】本実施形態におけるCPU20の動作領域としてのアクセス空間を示す図である。

【図11】本実施形態におけるCPU20の動作領域としてのコマンド空間を示す図である。

【図12】本実施形態におけるCPU20の動作領域としてのOS空間およびコマンド空間を示す図である。

【図13】本実施形態におけるCPU20の動作領域としてのアクセス空間を示す図である。

10 【図14】本実施形態におけるCPU20の動作領域としてのコマンド空間を示す図である。

【図15】本実施形態におけるICカードのライフサイクルを示す図である。

【図16】本実施形態におけるICカード発行の際の本人の認証を行なう手法を示す図である。

【図17】本実施形態におけるICカード発行の際の本人の認証を行なう手法を示す図である。

【図18】本実施形態におけるプロテクションフラグの設定手法を説明するための図である。

20 【図19】本実施形態におけるICカード利用による動作を説明するためのブロック図である。

【図20】本実施形態におけるICカード利用による動作を説明するためのブロック図である。

【図21】本実施形態におけるICカード利用による動作を説明するためのブロック図である。

【図22】本実施形態におけるICカード利用による動作を説明するためのブロック図である。

【図23】ICカードのハードウェア構成を示すブロック図である。

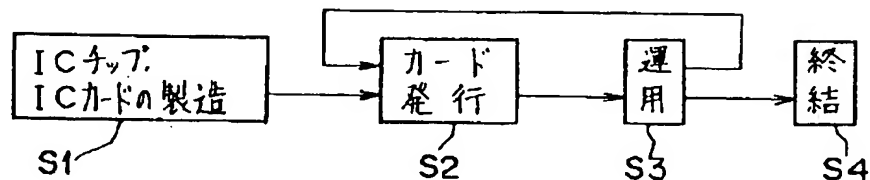
【符号の説明】

- 30 1 ICカード
2 メモリ領域
3 実行処理機構
4 受付機構
5 領域制御機構
5A 領域テーブル
6 領域監視機構
10 ICカード
11 ATM装置
12 端末
40 13 証明書発行機
14 医療機
15, 16 カード発行装置
20 CPU
21 命令実行部
22 受付部
23 領域制御部
23a 空間テーブル（領域テーブル）
23a-1 共用空間テーブル
23a-2, 23a-3 アドレステーブル
50 24 領域監視部

37	38
24 a コントロールレジスタ	51 テーブルポイント情報
30 メモリ	52 アクセス空間領域情報
30 A 統括制御領域	52 a 共用データ空間情報
30 B データ領域	52 b 共用アクセス制御空間情報
30 C プログラム領域	53 テーブルポイント情報
31 OS空間	54 空間モード設定部
32 アクセス空間	55 ステータス設定部
32 B-1~32 B-3 領域	56 共用空間領域設定部
33 コマンド空間	57 空間領域設定部
33 C-1~33 C-31 領域	10 60 本人認証カード
34 プロテクションフラグ領域	61 ステータス情報
35 プロテクションフラグ	62 認証データ
40, 40 A 上位装置	63 アプリケーション識別用情報
41 ID情報	64, 65 認証情報
42 ポイント情報	66 認証情報テーブル
43 ステータス情報	72 アクセス空間
44 認証情報	72 B 共用アクセス空間
45 コマンド空間領域情報	73 コマンド空間
45 a コマンド空間情報	73 A 拡張コマンド空間
45 b 拡張コマンド空間情報	20 73 B 共用コマンド空間
46 テーブルポイント情報	73 C 共用拡張コマンド空間
47 アクセス空間領域情報	100 ICカード
47 a データ空間情報	101 CPU
47 b アクセス制御空間情報	101 a ROM
48 テーブルポイント情報	101 b RAM
49 認証情報	101 c 制御部
50 コマンド空間領域情報	101 d 決算部
50 a 共用コマンド空間情報	102 コネクト部
50 b 共用拡張コマンド空間情報	103 メモリ

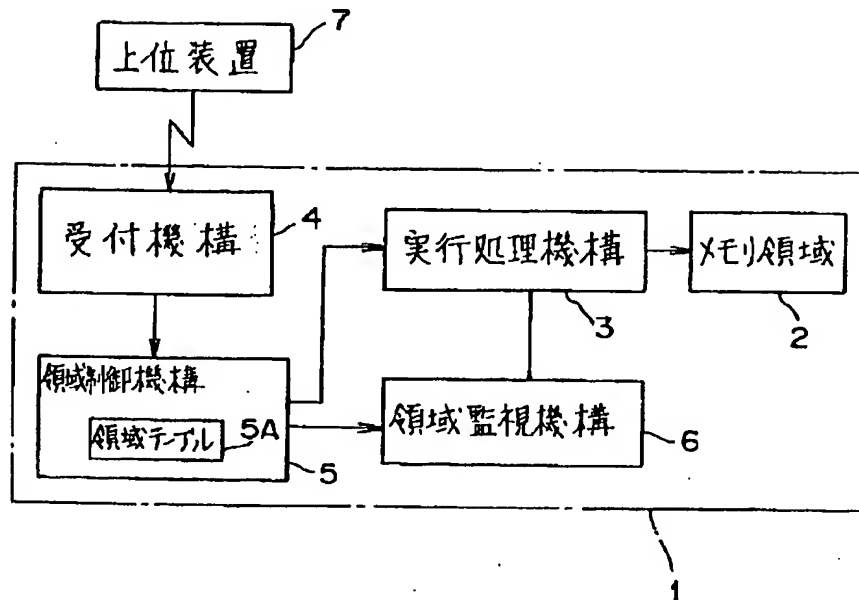
【図15】

本実施形態におけるICカードのライフサイクルを示す図



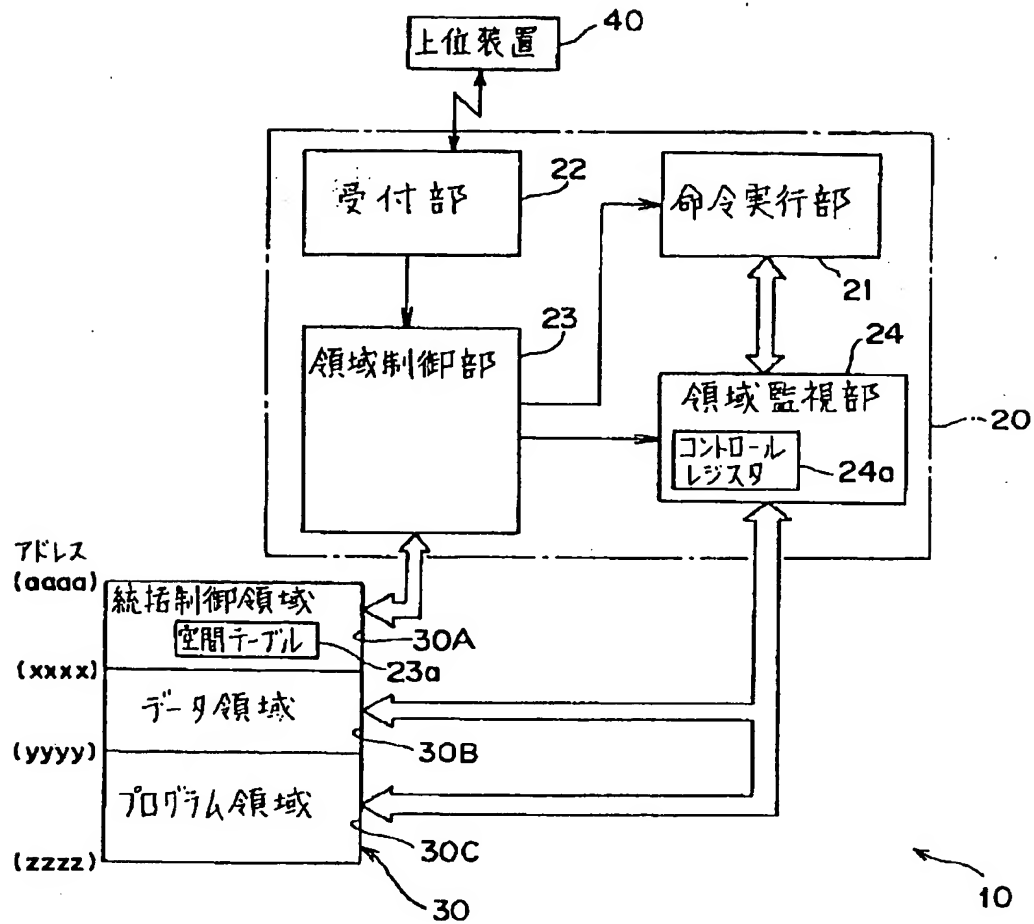
【図1】

本発明の原理ブロック図



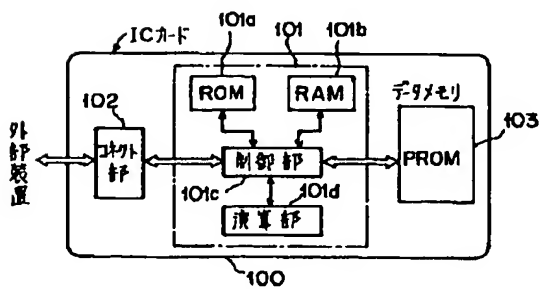
【図2】

本発明の一実施形態にかかるICカードを示すブロック図



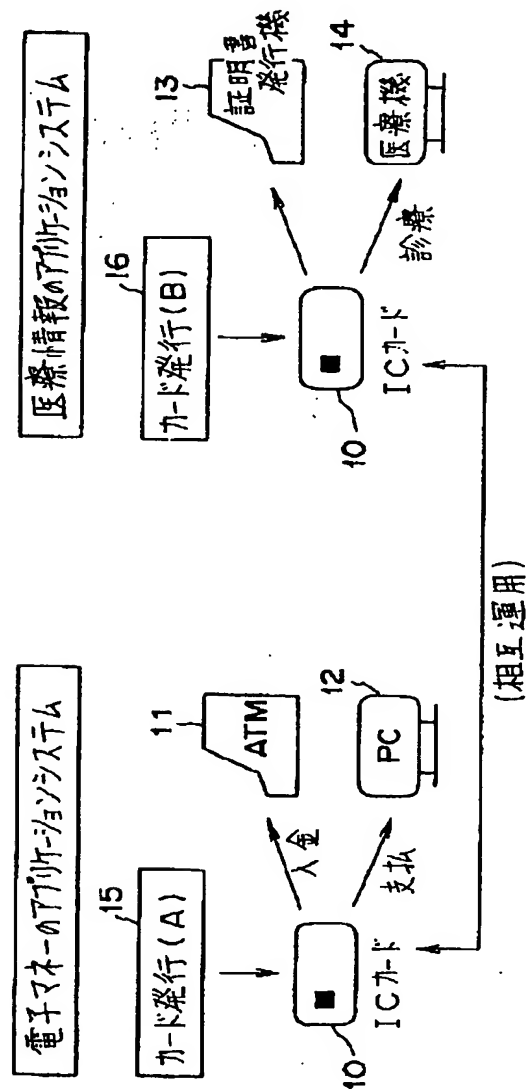
【図23】

ICカードハードウェア構成を示すブロック図



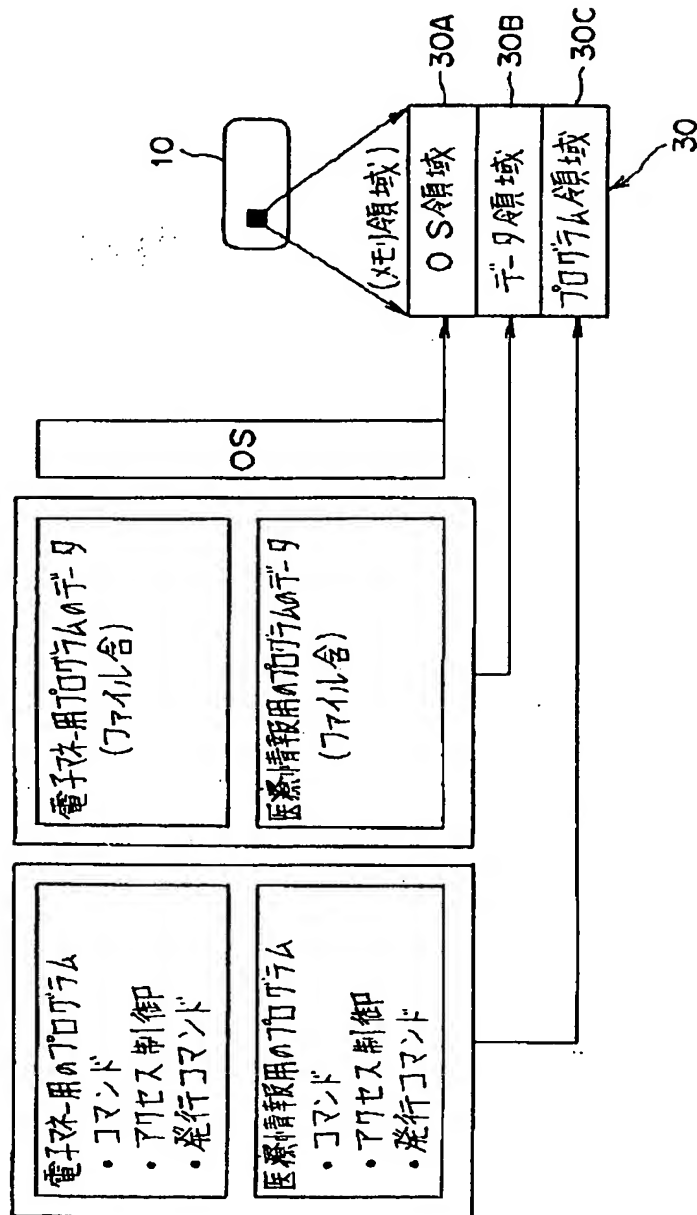
【図3】

本実施形態にかかる各種アプリケーションシステムを実現するICカードの
上位装置への接続態様を示す図



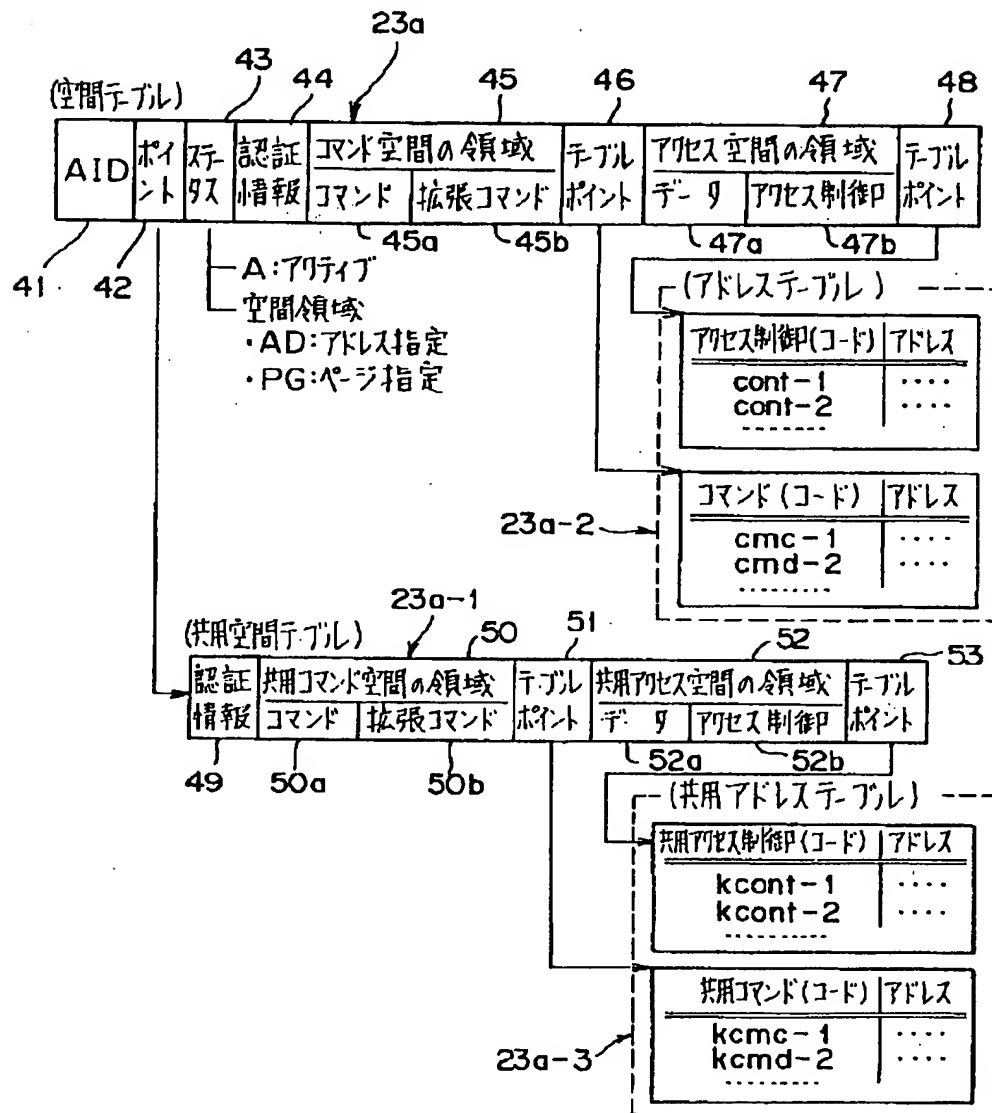
【図4】

本実施形態における各アプリケーションのプログラムやデータが記憶される領域を説明するための図



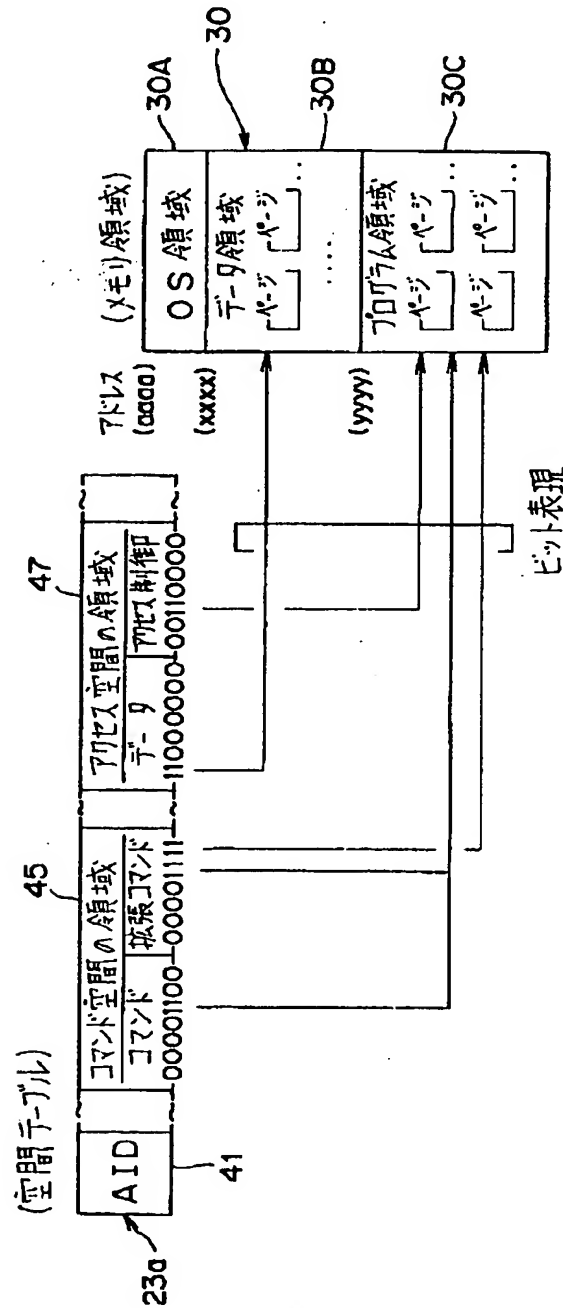
【図5】

本実施形態における領域制御部に参照される空間テーブルを示す図



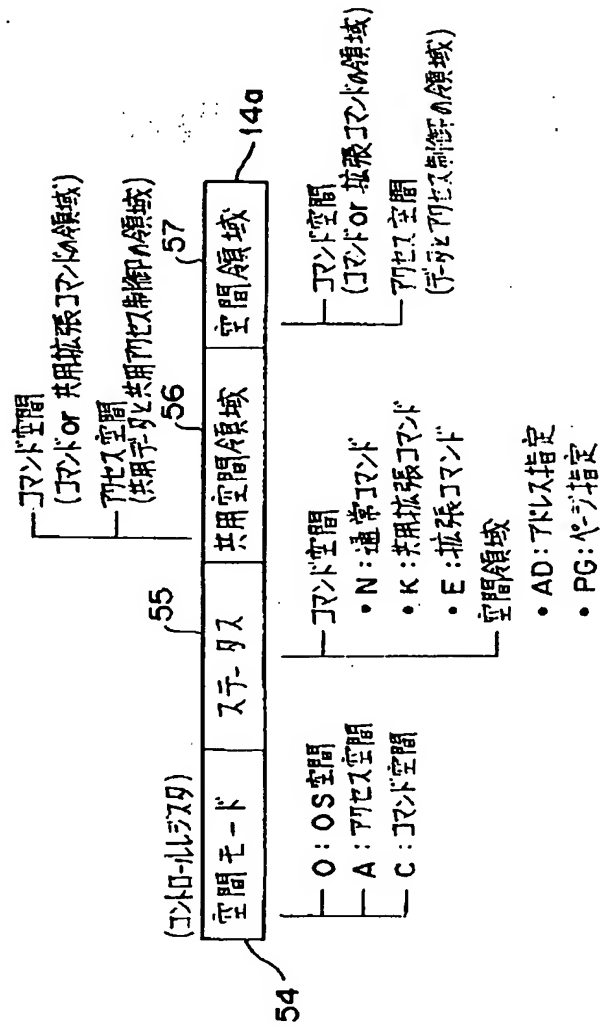
【図6】

本実施形態における領域制御部にて参照される空間テーブルの
要部を示す図



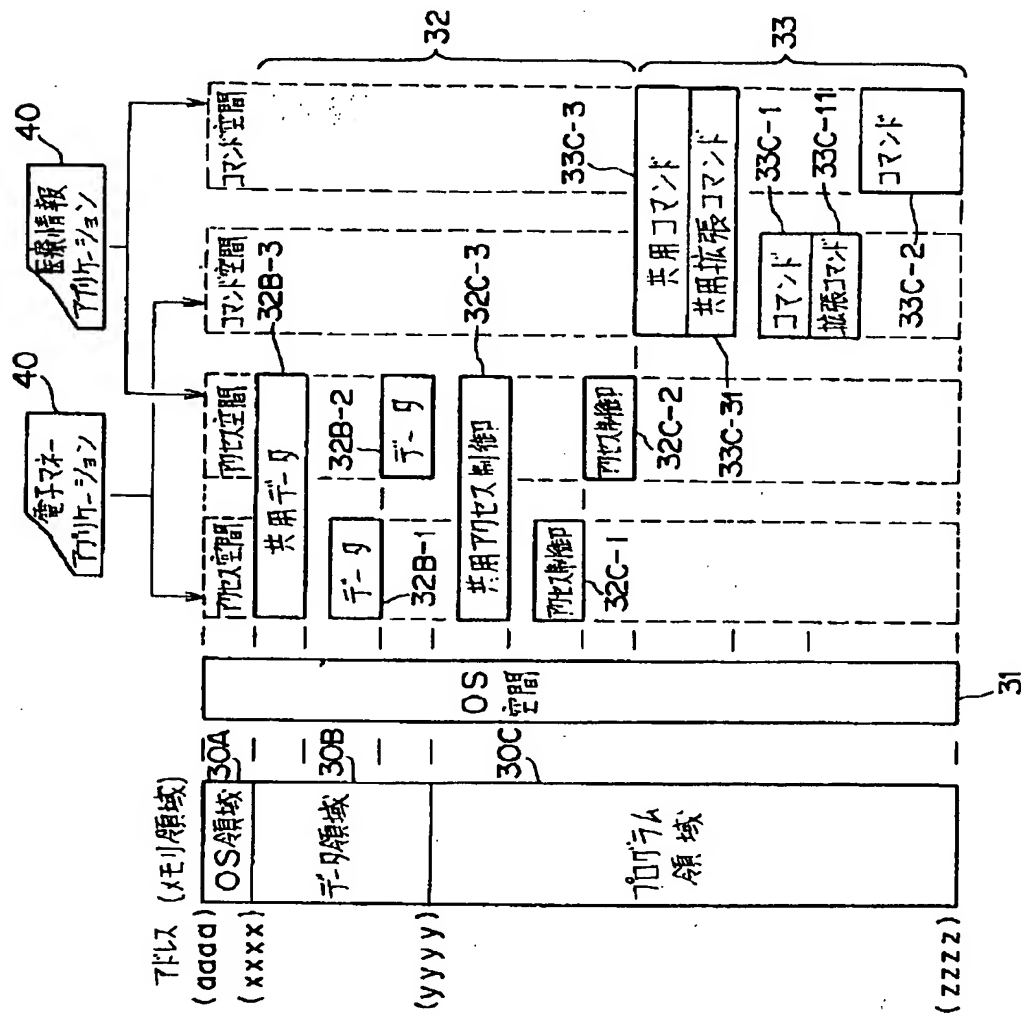
【図7】

本実施形態における領域監視部のコントロールリストに設定される情報を示す図



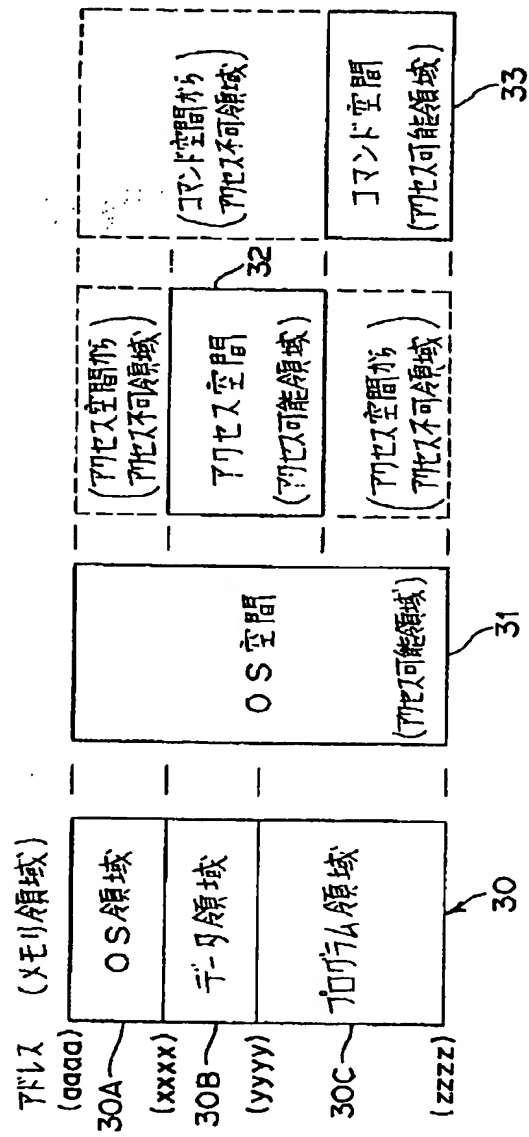
【図8】

本実施形態におけるCPU 20の動作領域としてのOS空間、アドレス空間およびコマンド空間を示す図



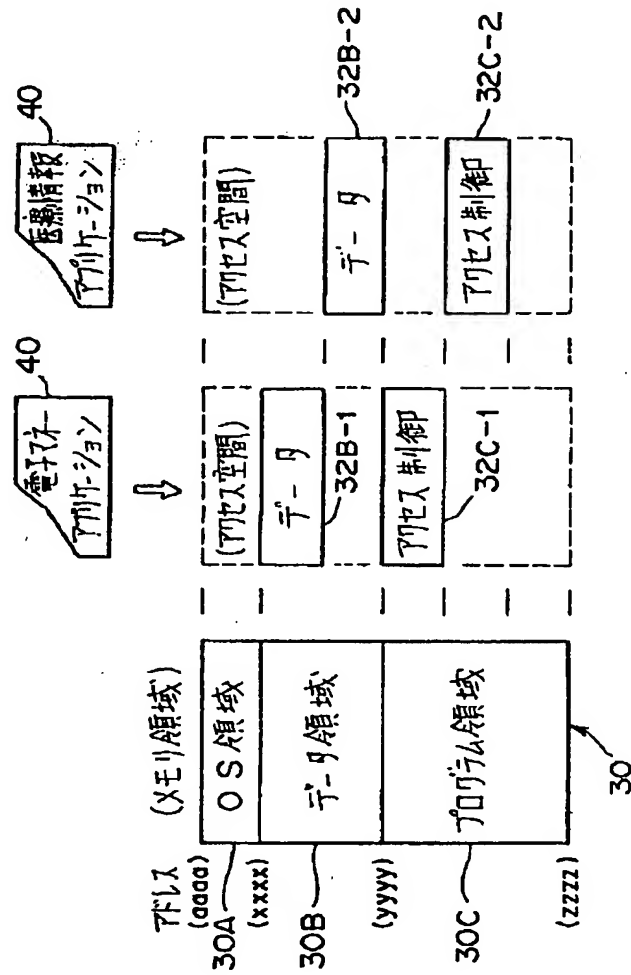
【図9】

本実施形態におけるCPU 20 の動作領域としてのOS 空間、
アクセス空間およびコマンド空間を示す図



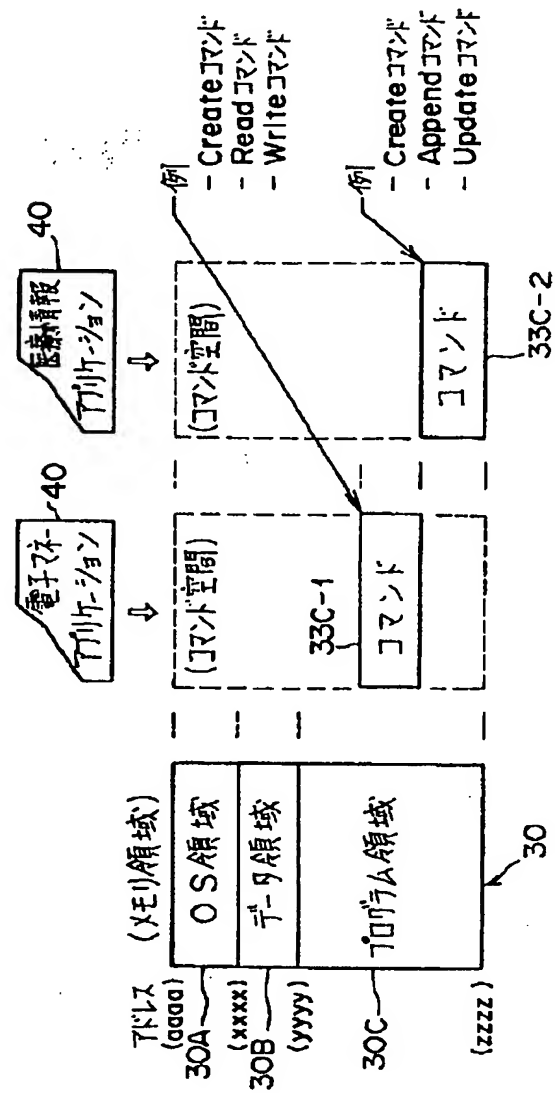
【図10】

本実施形態におけるCPU20の動作領域としての
アクセス空間を示す図



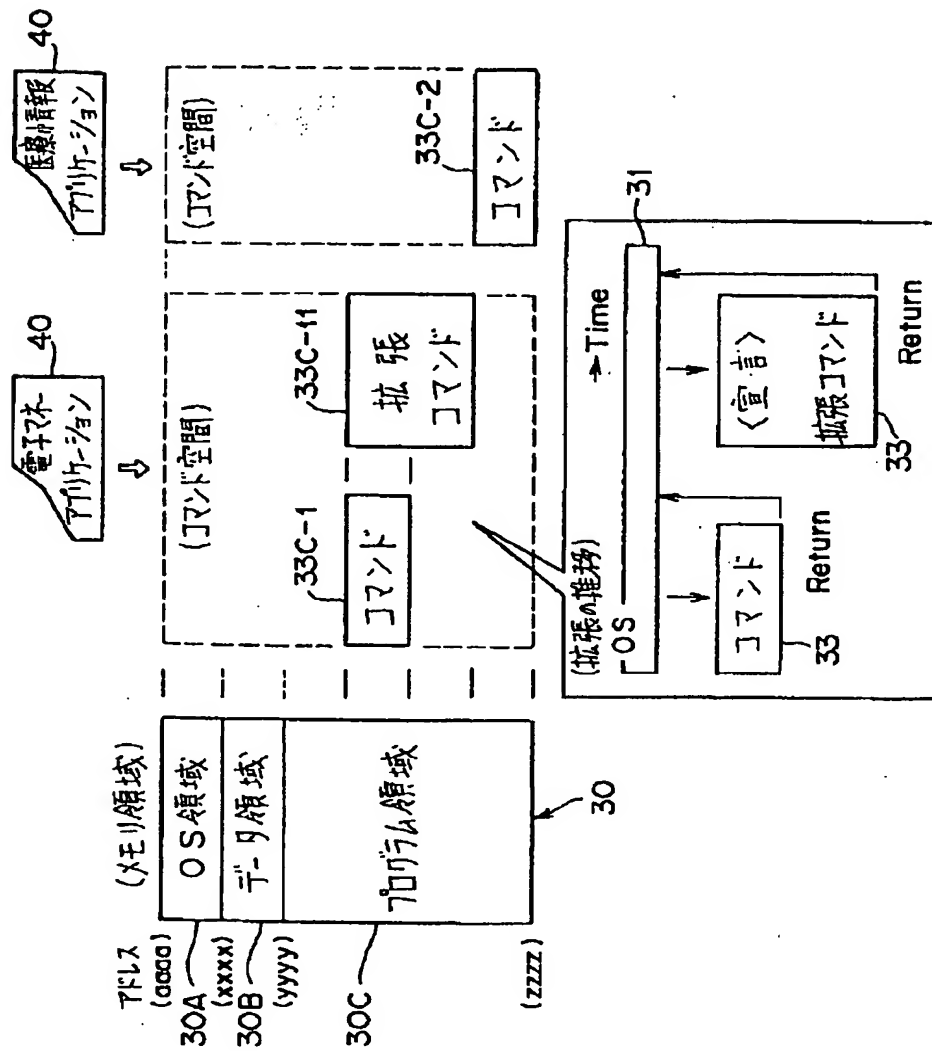
【図11】

本実施形態におけるCPU 20の動作領域としての
コマンド空間を示す図



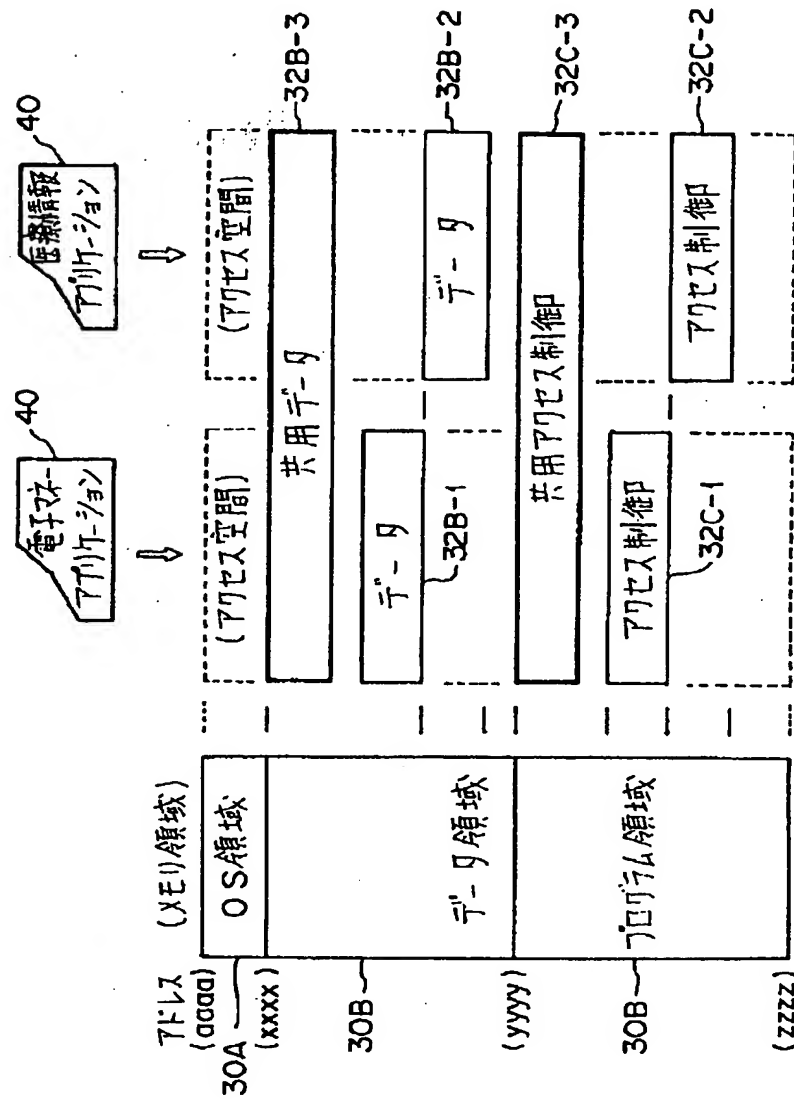
【図12】

本実施形態におけるCPU20の動作領域としてのOS空間およびコマンド空間を示す図



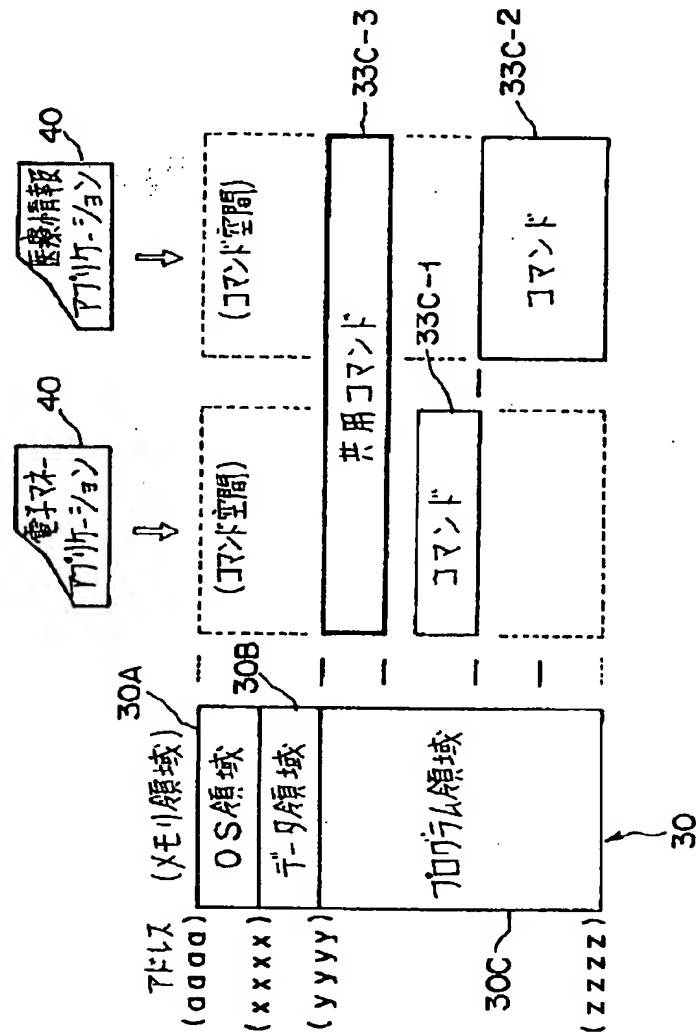
【図13】

本実施形態におけるCPU20の動作領域としての
アドレス空間を示す図



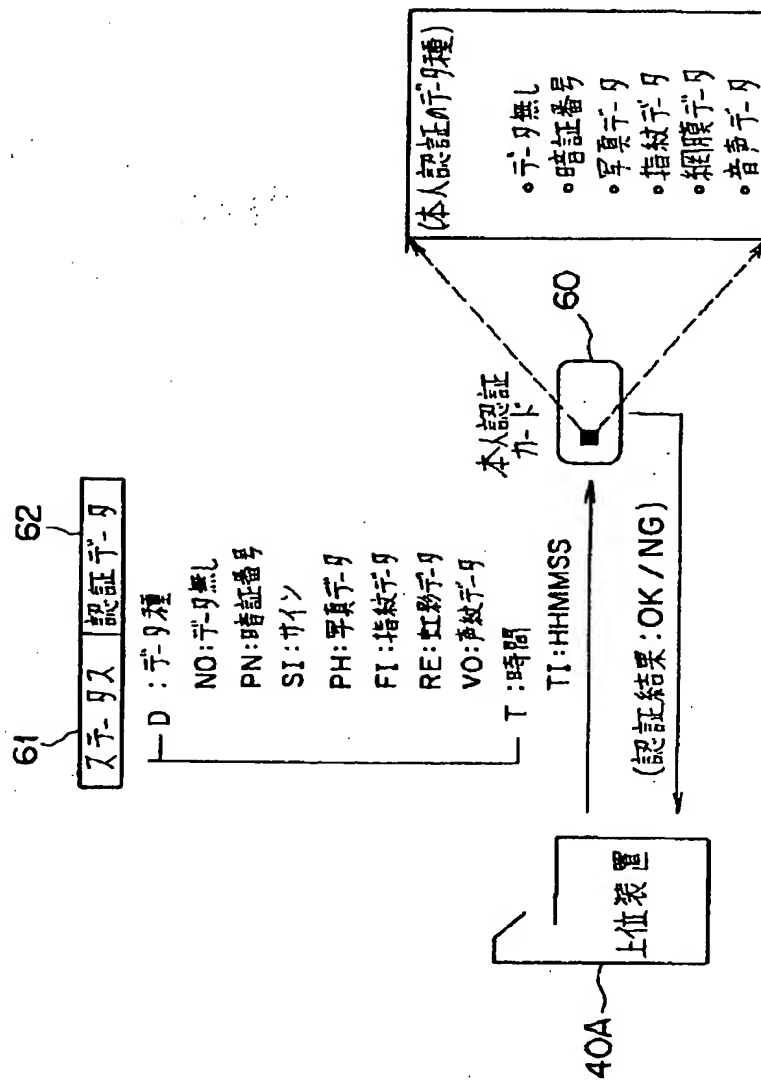
【図14】

本実施形態におけるCPU20の動作領域としての
コマンド空間を示す図



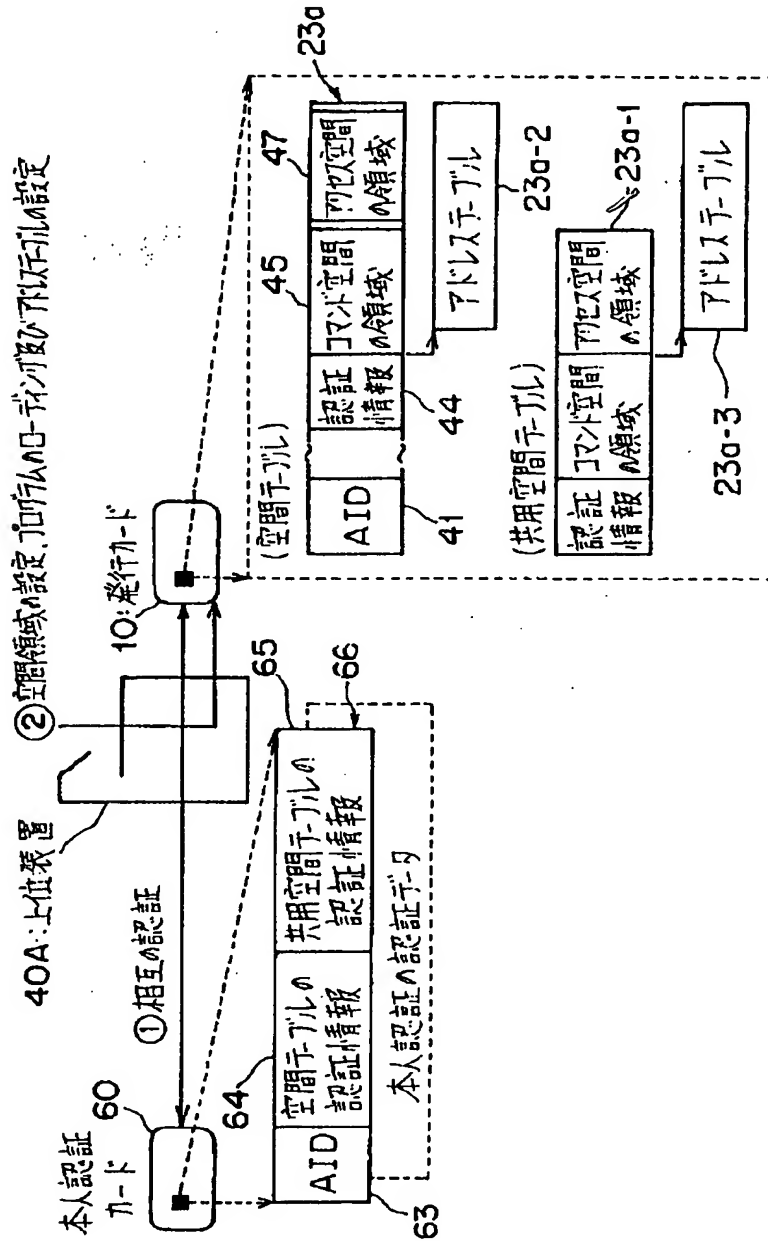
【図16】

本実施形態におけるICカード発行の際の本人の認証を行なう手法を示す図



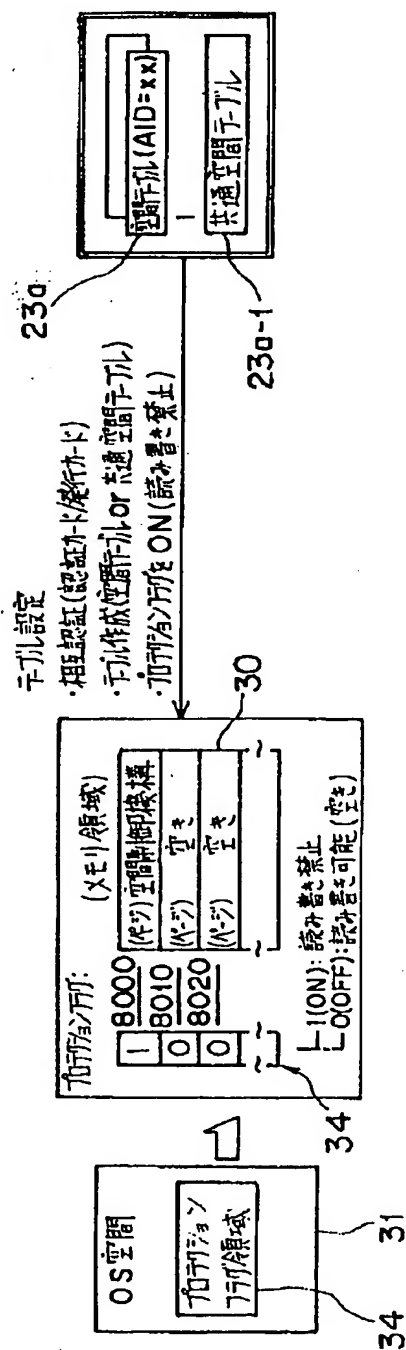
【図17】

本実施形態におけるICカード発行の際の本人の認証を行なう手法を示す図



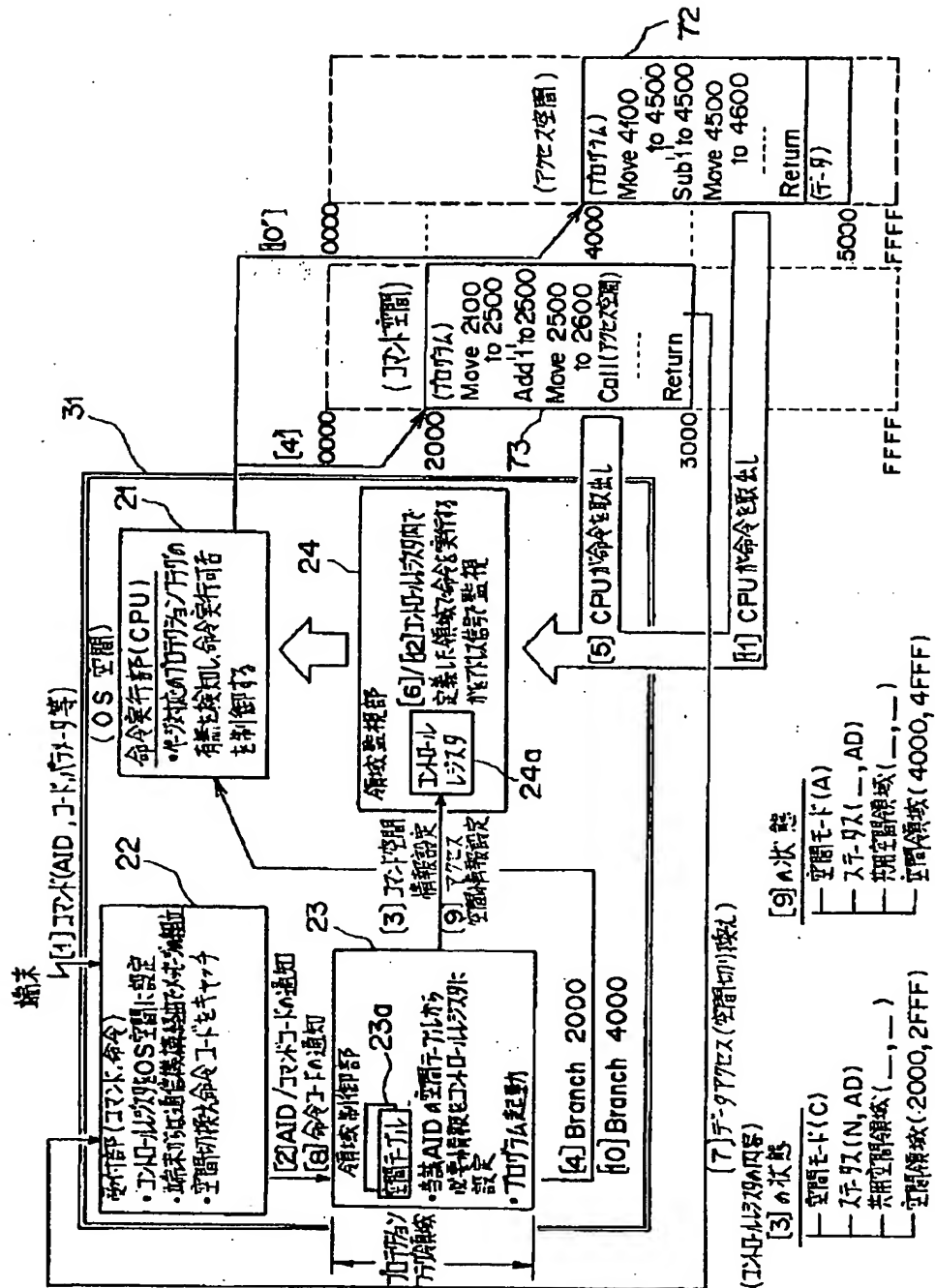
【図18】

本実施形態におけるプロテクションラジの設定手法を説明するための図



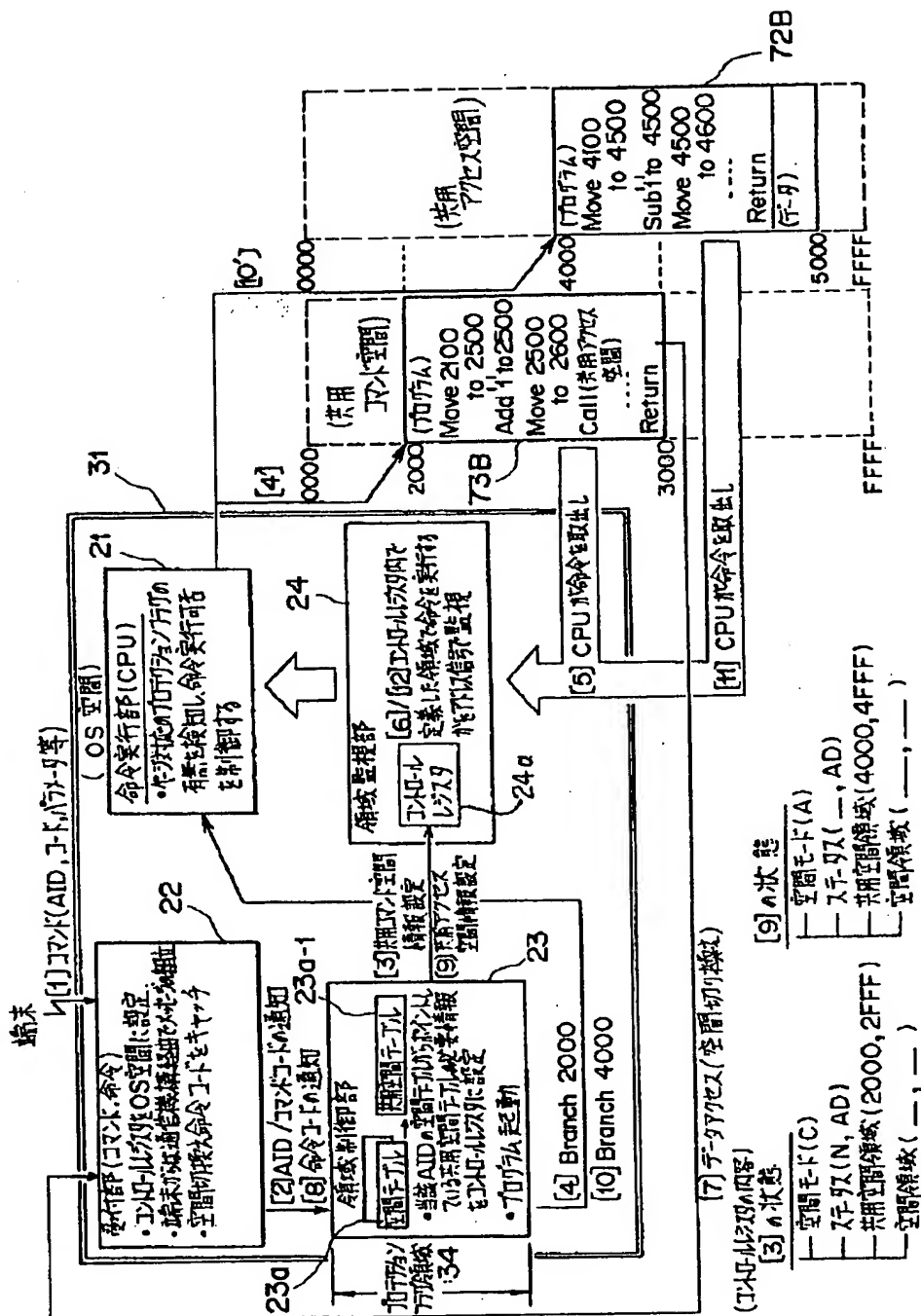
【図19】

本実施形態におけるICカード利用による動作を説明するためのブロック図



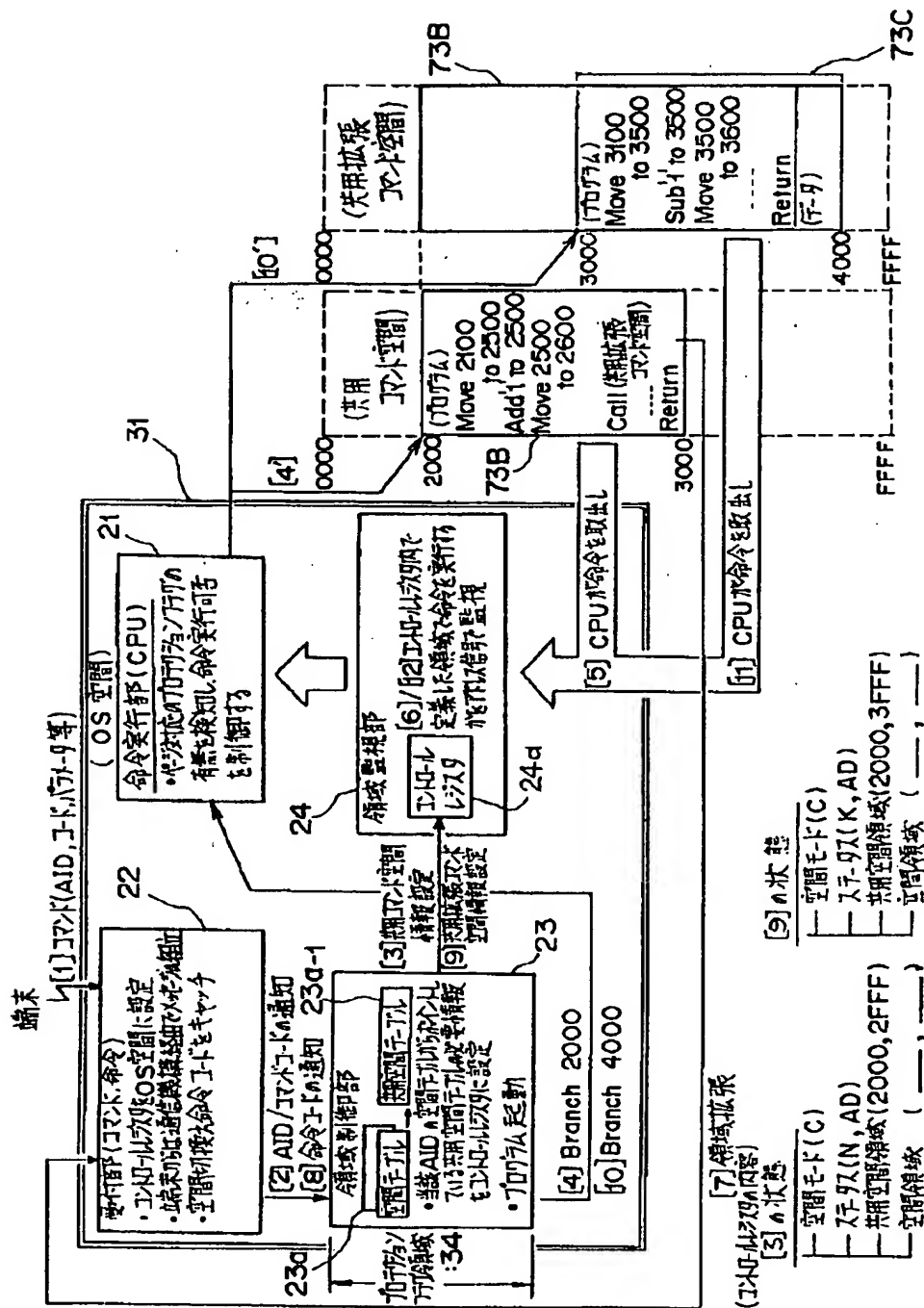
【図21】

本実施形態におけるIC カード利用による動作を説明するためのブロック図



【図22】

本実施形態におけるICカード利用による動作を説明するためのブロック図



フロントページの続き

(54) 【発明の名称】 可搬型カード媒体、可搬型カード媒体のメモリ空間管理方法、可搬型カード媒体の発行方法および可搬型カード媒体のプログラムデータ書込方法並びにメモリ空間管理プログラムが記録された

コンピュータ読取可能な記録媒体